ASA 8.2: Port Redirection (Forwarding) mit nat-, global, statischen und Zugriffslistenbefehlen mithilfe von ASDM

Inhalt

Einführung

Dieses Dokument beschreibt die Funktionsweise der Port-Umleitung auf der Cisco Adaptive Security Appliance (ASA) mit ASDM. Es befasst sich mit der Zugriffskontrolle für den Datenverkehr über die ASA und der Funktionsweise von Übersetzungsregeln.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- NAT-Übersicht
- PIX/ASA 7.X: Port-Umleitung

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco ASA der Serie 5500, Version 8.2
- Cisco ASDM Version 6.3

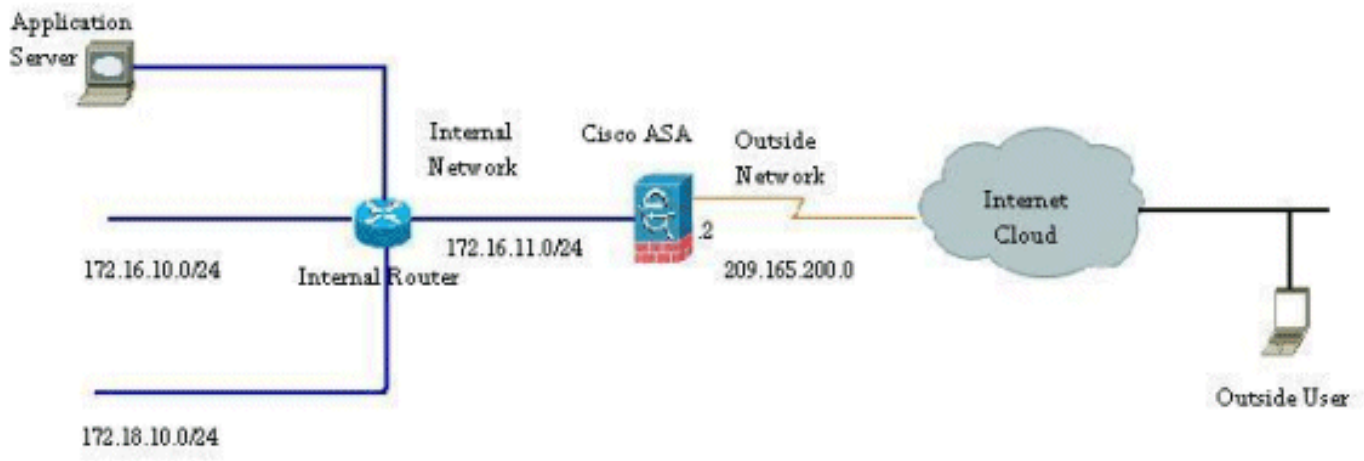
Hinweis: Diese Konfiguration funktioniert nur von der Cisco ASA-Software Version 8.0 bis 8.2 einwandfrei, da die NAT-Funktionalität nicht wesentlich verändert wird.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Netzwerkdiagramm



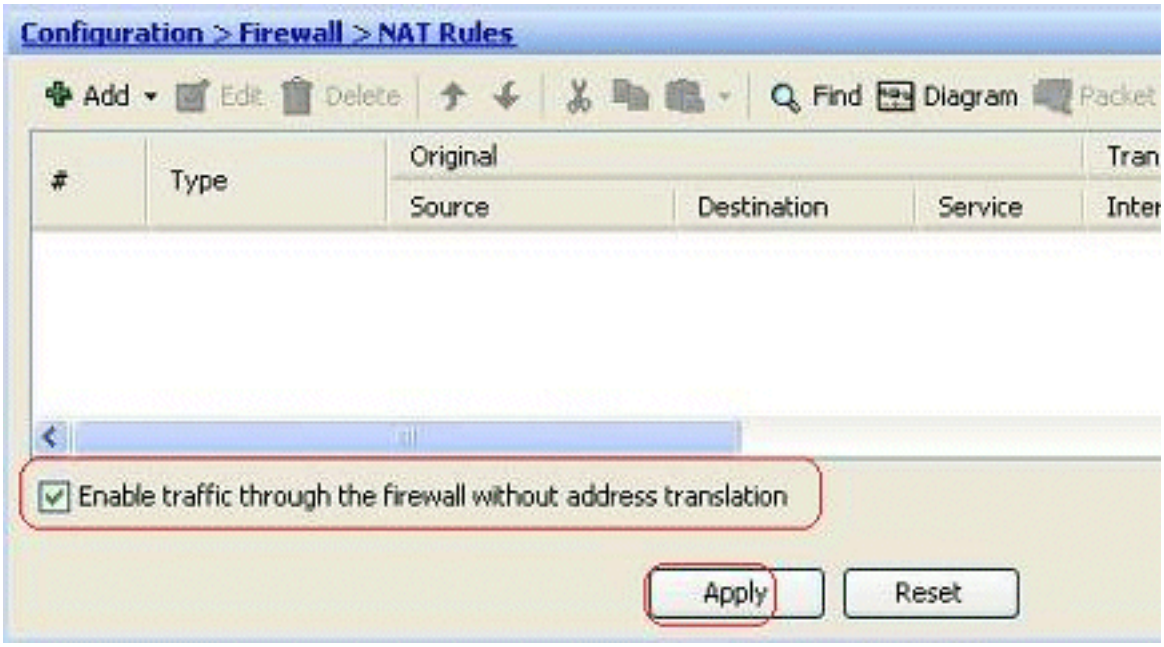
Die in dieser Konfiguration verwendeten IP-Adressierungsschemata sind im Internet nicht rechtlich routbar. Es handelt sich um RFC 1918-Adressen, die in einer Laborumgebung verwendet wurden.

Ausgehenden Zugriff zulassen

Der ausgehende Zugriff beschreibt Verbindungen von einer Schnittstelle mit höherer Sicherheitsstufe zu einer Schnittstelle mit niedrigerer Sicherheitsstufe. Dazu gehören Verbindungen von innen nach außen, von innen nach Demilitarized Zones (DMZs) und von DMZs nach außen. Dies kann auch Verbindungen von einer DMZ zu einer anderen umfassen, sofern die Schnittstelle der Verbindungsquelle eine höhere Sicherheitsstufe als das Ziel hat.

Ohne eine konfigurierte Übersetzungsregel kann keine Verbindung die Sicherheits-Appliance passieren. Diese Funktion wird als NAT-Control bezeichnet. Das hier abgebildete Bild zeigt, wie diese Funktion über ASDM deaktiviert wird, um Verbindungen über die ASA ohne

Adressübersetzung zu ermöglichen. Wenn Sie jedoch eine Übersetzungsregel konfiguriert haben, bleibt die Deaktivierung dieser Funktion für den gesamten Datenverkehr ungültig und Sie müssen die Netzwerke explizit von der Adressübersetzung ausnehmen.

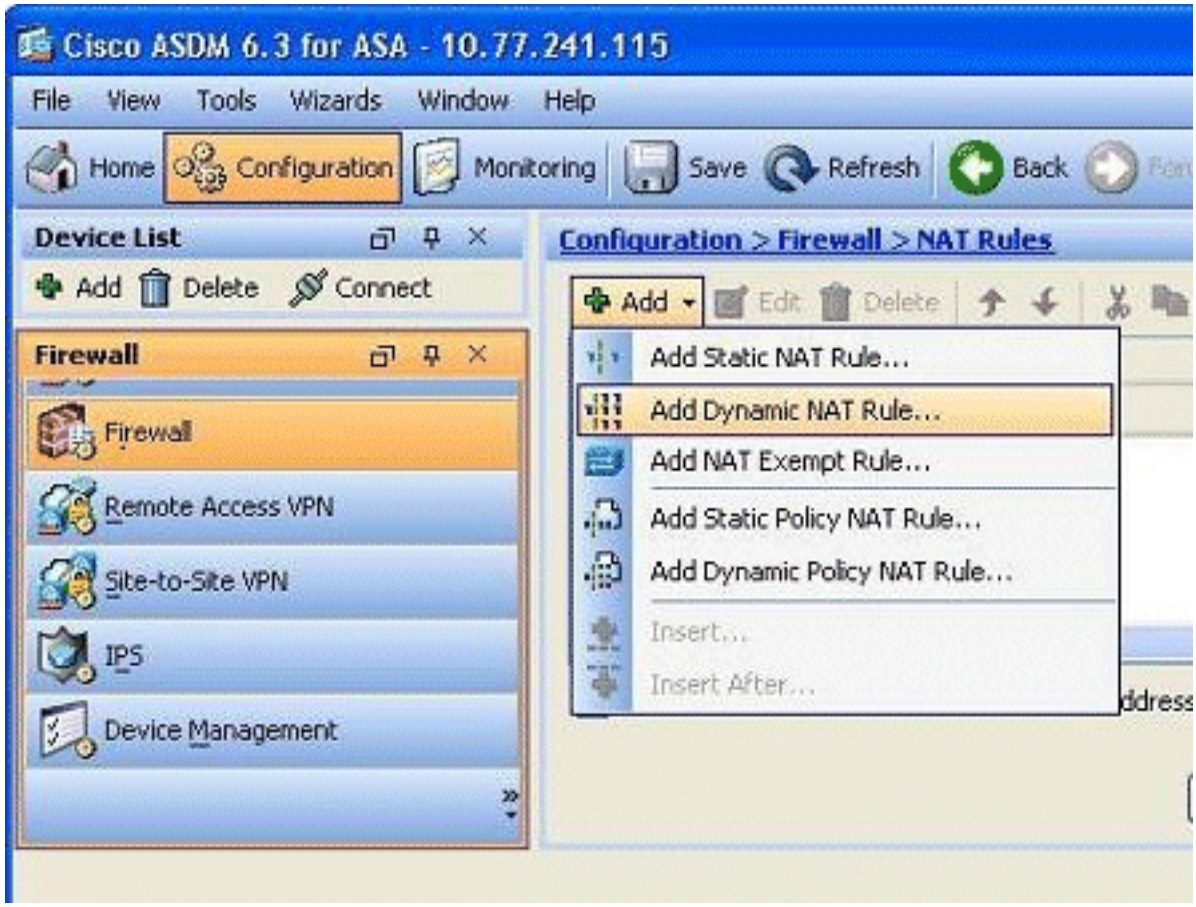


Zugriff für interne Hosts auf externe Netzwerke mit NAT zulassen

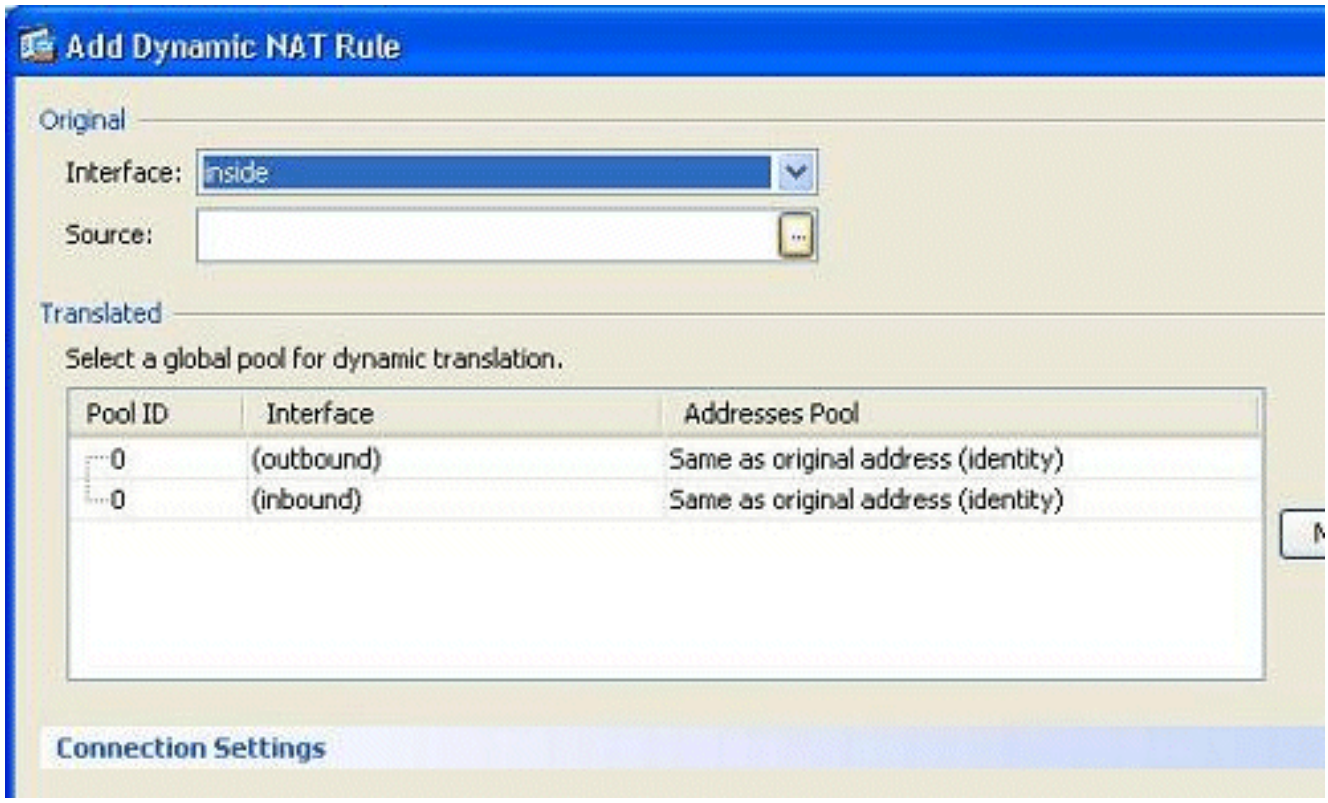
Sie können einer Gruppe von internen Hosts/Netzwerken den Zugriff auf die Außenwelt ermöglichen, indem Sie die dynamischen NAT-Regeln konfigurieren. Um dies zu erreichen, müssen Sie die tatsächliche Adresse der Hosts/Netzwerke auswählen, die Zugriff erhalten sollen. Diese müssen dann einem Pool übersetzter IP-Adressen zugeordnet werden.

Gehen Sie wie folgt vor, um internen Hosts den Zugriff auf externe Netzwerke mit NAT zu ermöglichen:

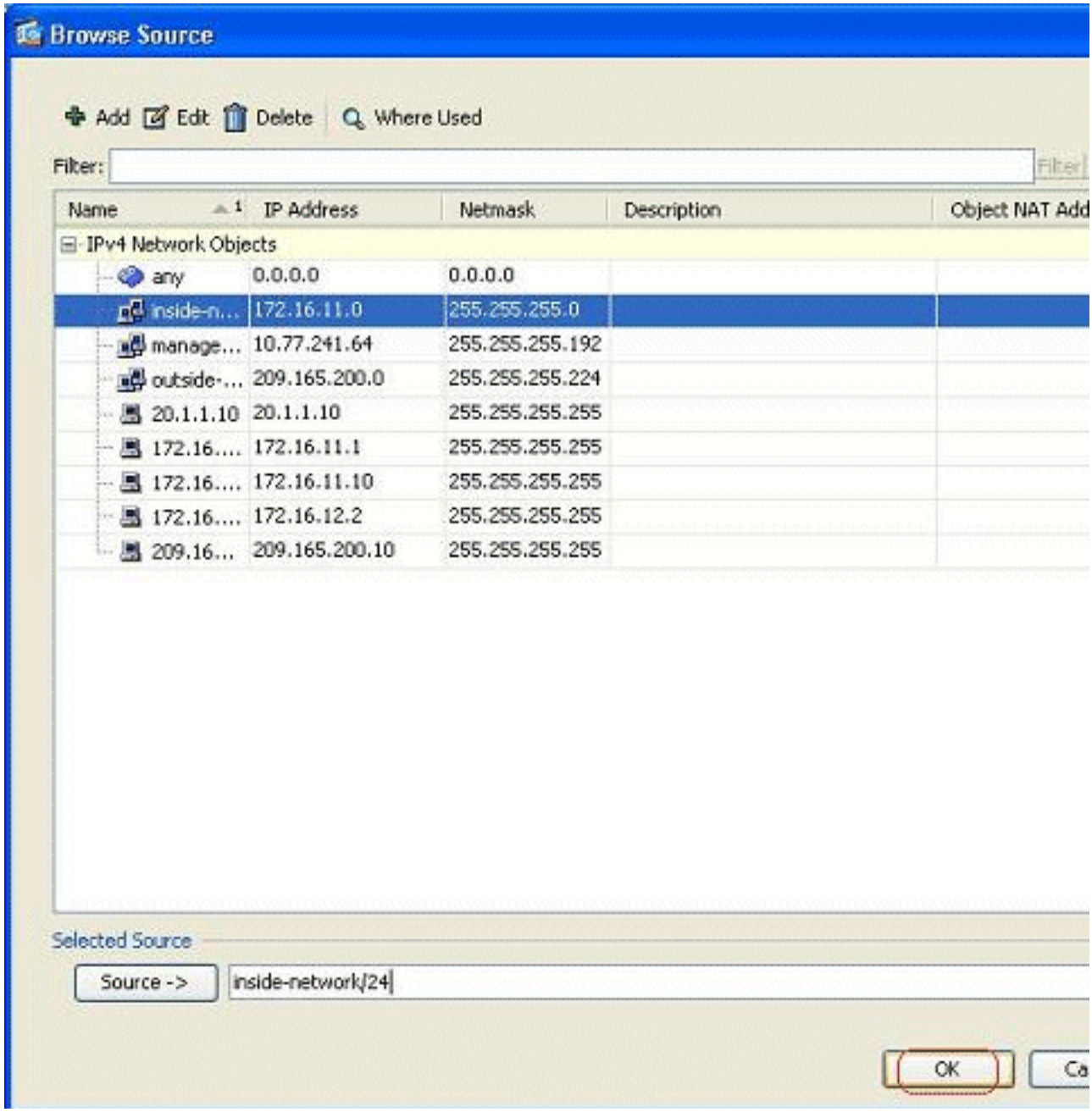
1. Gehen Sie zu **Konfiguration > Firewall > NAT Rules**, klicken Sie auf **Hinzufügen**, und wählen Sie dann die **Option Dynamische NAT-Regel hinzufügen aus, um eine dynamische NAT-Regel zu konfigurieren.**



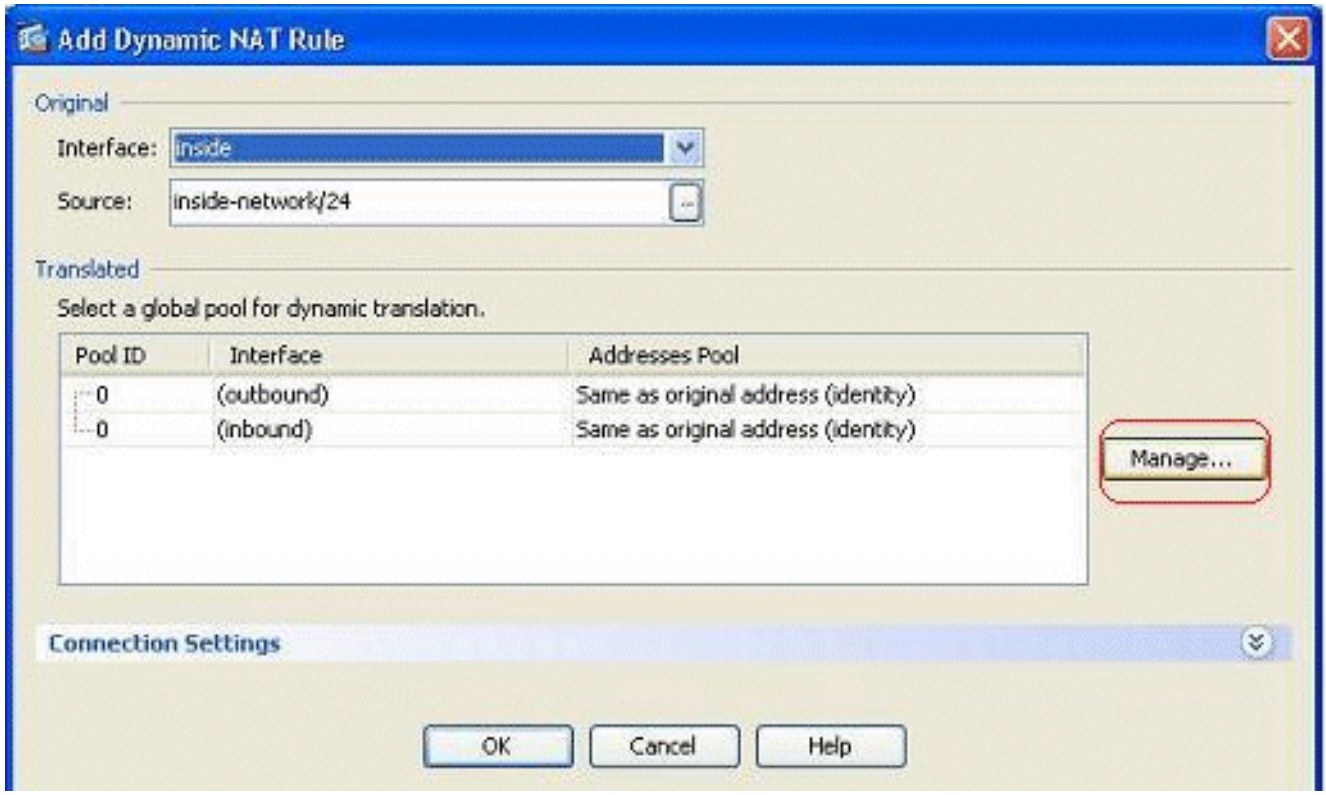
2. Wählen Sie den Namen der Schnittstelle aus, mit der die echten Hosts verbunden sind. Wählen Sie die tatsächliche IP-Adresse der Hosts/Netzwerke mithilfe der Schaltfläche **Details** im Feld **Quelle**
aus.



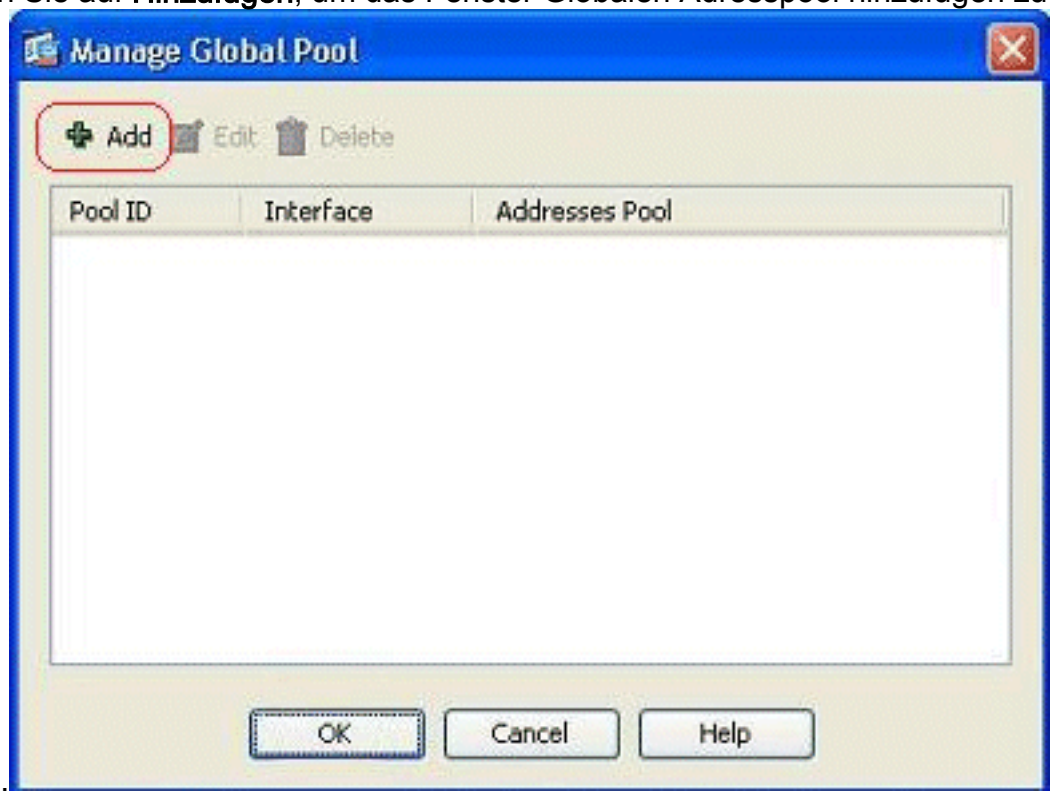
3. In diesem Beispiel wurde das gesamte *interne Netzwerk* ausgewählt. Klicken Sie auf **OK**, um die Auswahl
abzuschließen.



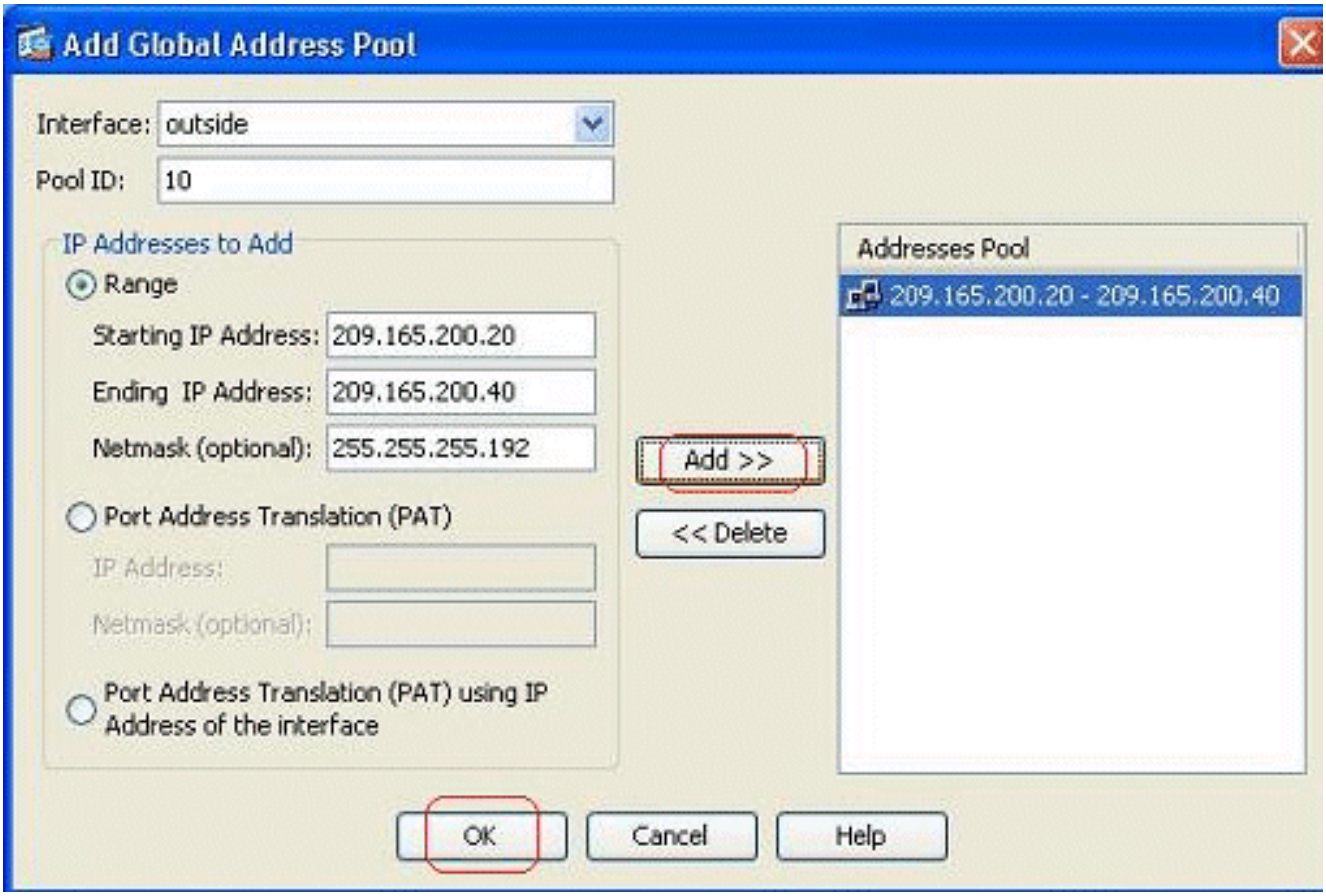
4. Klicken Sie auf **Verwalten**, um den Pool von IP-Adressen auszuwählen, dem das echte Netzwerk zugeordnet
wird.



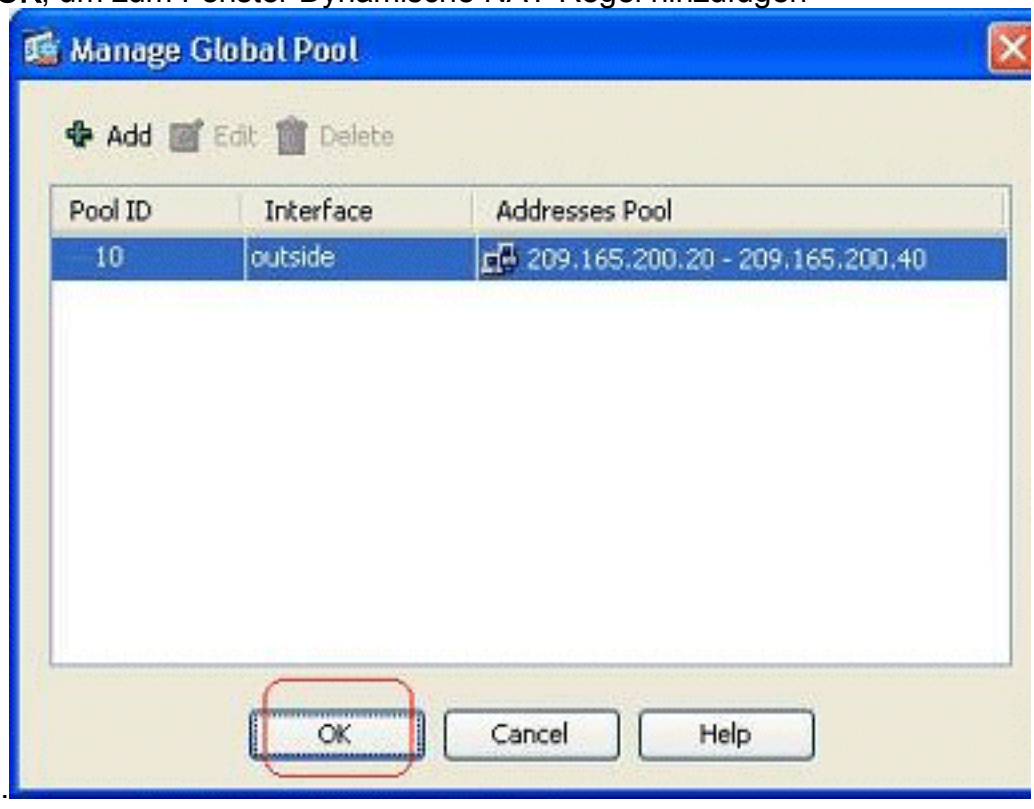
5. Klicken Sie auf **Hinzufügen**, um das Fenster Globalen Adresspool hinzufügen zu öffnen.



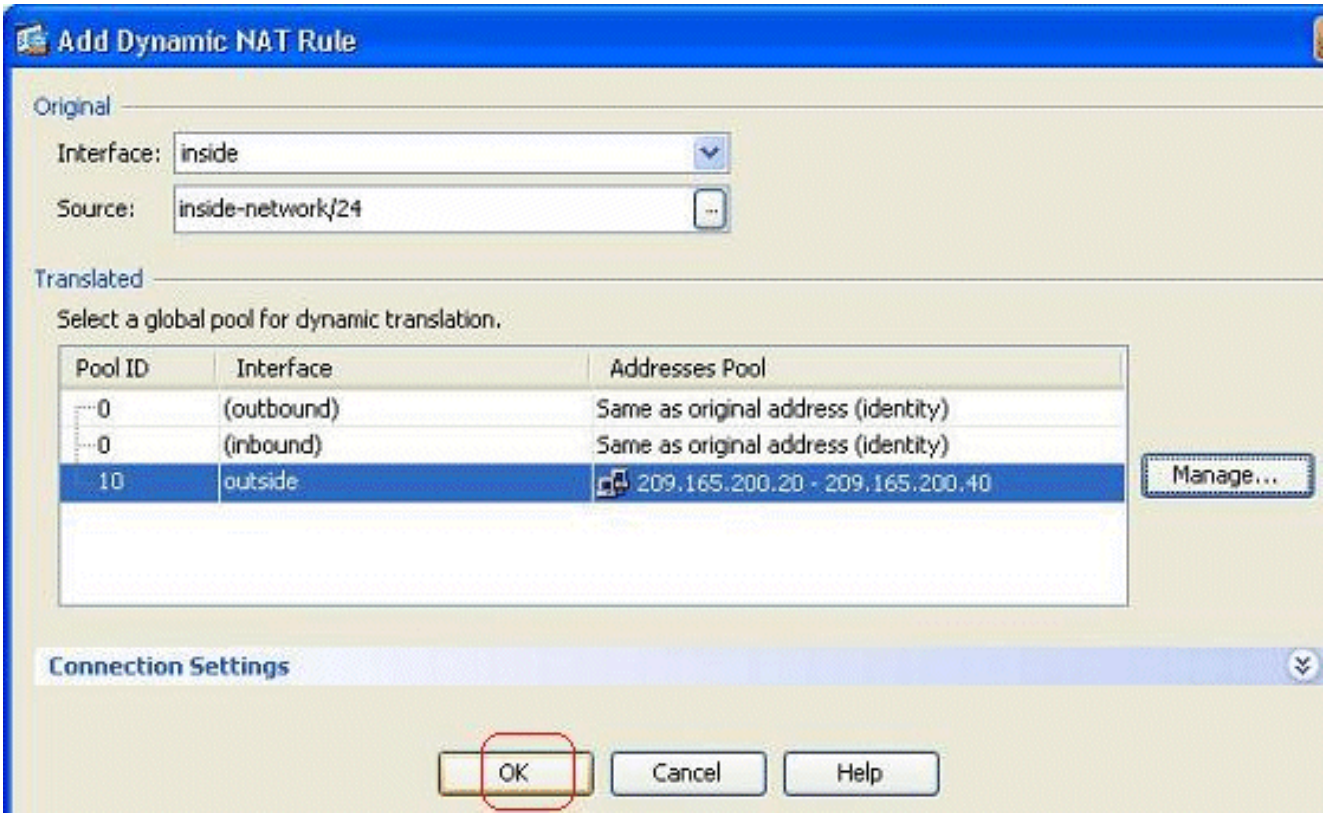
6. Wählen Sie die Option **Range (Bereich) aus**, und geben Sie die Start- und End-IP-Adressen zusammen mit der Ausgangsschnittstelle an. Geben Sie außerdem eine eindeutige Pool-ID an, und klicken Sie auf **Hinzufügen**, um diese dem Adresspool hinzuzufügen. Klicken Sie auf **OK**, um zum Fenster Globalen Pool verwalten zurückzukehren.



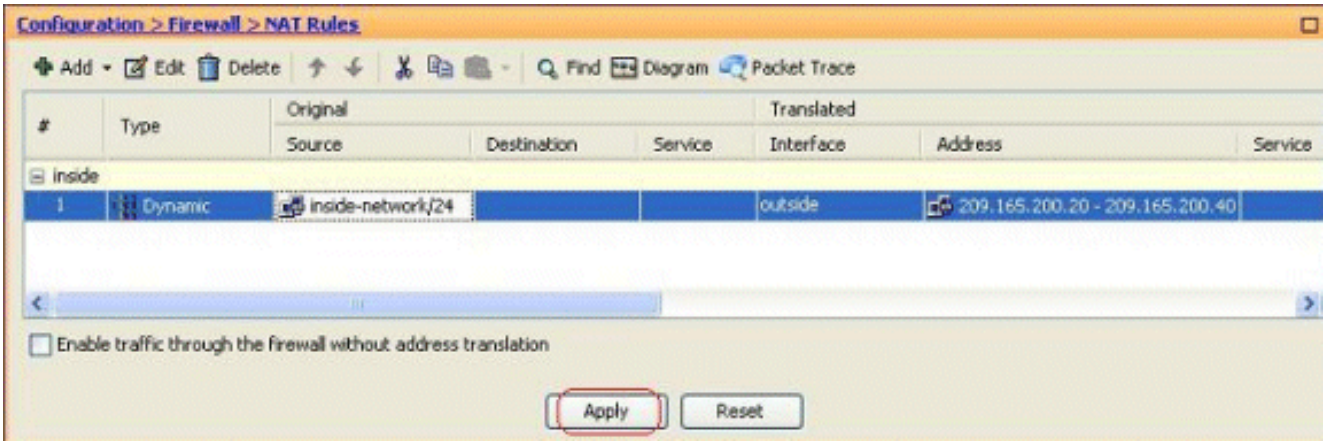
7. Klicken Sie auf **OK**, um zum Fenster Dynamische NAT-Regel hinzufügen zurückzukehren.



8. Klicken Sie auf **OK**, um die Konfiguration der dynamischen NAT-Regel abzuschließen.



9. Klicken Sie auf **Apply**, damit die Änderungen wirksam werden.**Hinweis:** Die Option **Verkehr durch die Firewall ohne Adressübersetzung aktivieren** ist deaktiviert.



Dies ist die entsprechende CLI-Ausgabe für diese ASDM-Konfiguration:

```
nat-control
global (outside) 10 209.165.200.20-209.165.200.40 netmask 255.255.255.192
nat (inside) 10 172.16.11.0 255.255.255.0
```

Gemäß dieser Konfiguration werden die Hosts im Netzwerk 172.16.11.0 in eine beliebige IP-Adresse aus dem NAT-Pool, 209.165.200.20-209.165.200.40, umgewandelt. Hier ist die NAT-Pool-ID sehr wichtig. Sie können denselben NAT-Pool einem anderen internen/DMZ-Netzwerk zuweisen. Wenn der zugeordnete Pool weniger Adressen als die reale Gruppe hat, könnten Ihnen Adressen fehlen, wenn der Datenverkehr die erwartete Menge übersteigt. Als Ergebnis könnten Sie versuchen, PAT zu implementieren, oder Sie könnten versuchen, den vorhandenen Adresspool zu bearbeiten, um ihn zu erweitern.

Hinweis: Beachten Sie, dass Sie die vorhandene Übersetzungsregel ändern müssen, damit **diese Änderungen wirksam werden**, jedoch den Befehl **clear xlate** **verwenden müssen**. Andernfalls

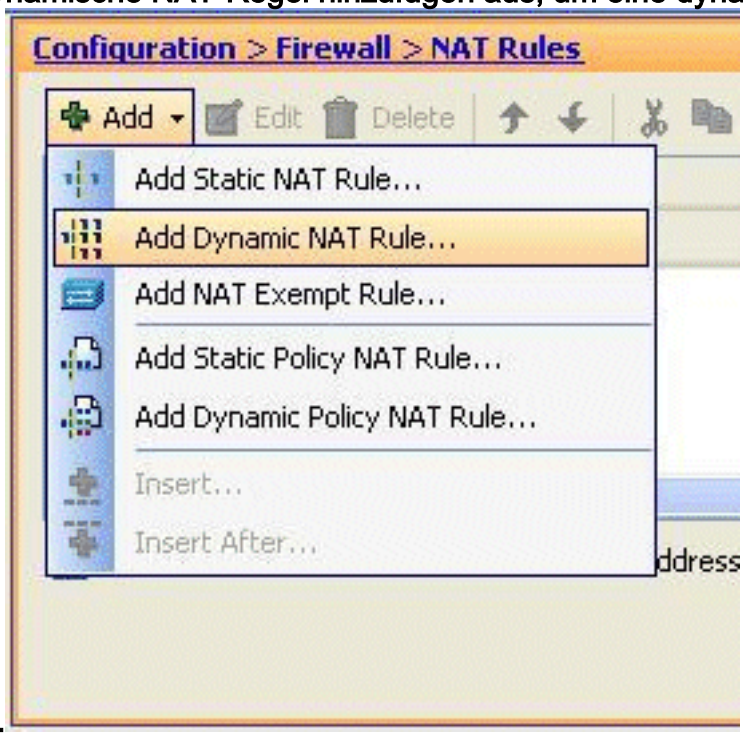
verbleibt die vorherige bestehende Verbindung in der Verbindungstabelle, bis sie das Timeout erreicht hat. Seien Sie vorsichtig, wenn Sie den Befehl **clear xlate** verwenden, da er die vorhandenen Verbindungen sofort beendet.

Zugriff für interne Hosts auf externe Netzwerke mit PAT zulassen

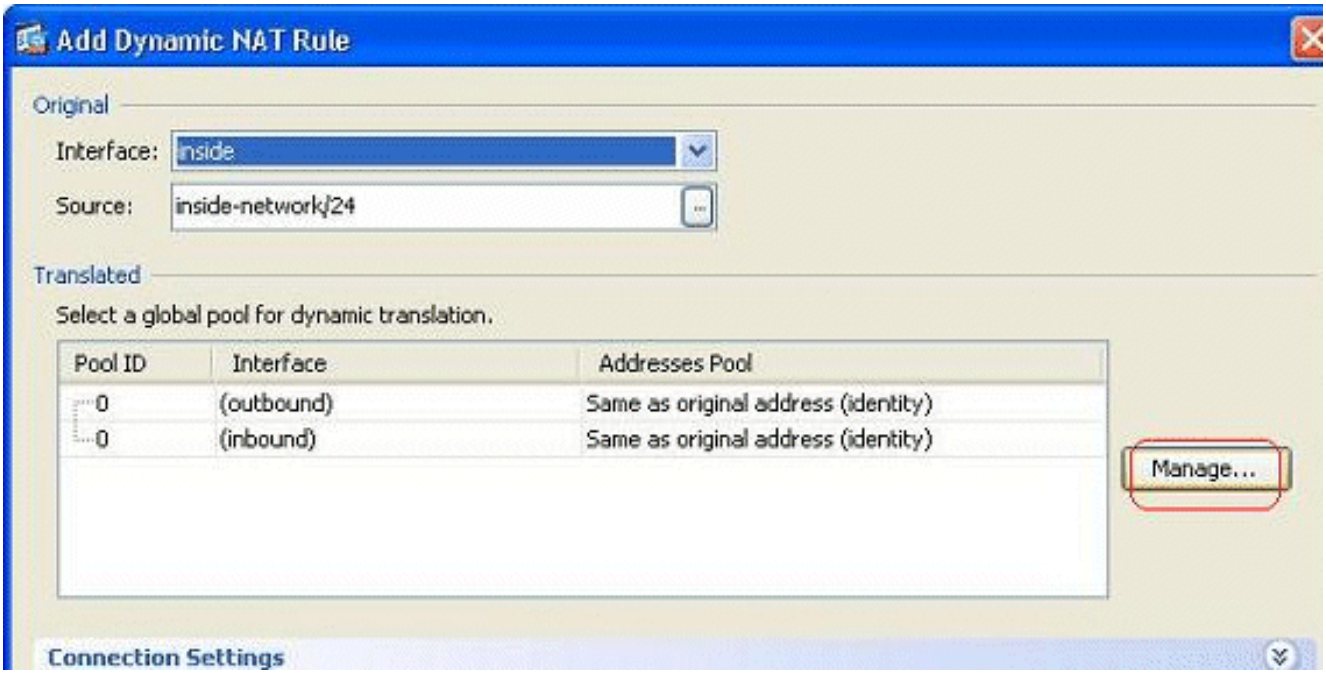
Wenn interne Hosts eine einzige öffentliche Adresse für die Übersetzung freigeben möchten, verwenden Sie PAT. Wenn die **globale** Anweisung eine Adresse angibt, wird diese Adresse vom Port übersetzt. Die ASA ermöglicht eine Port-Übersetzung pro Schnittstelle, und die Übersetzung unterstützt bis zu 65.535 aktive **Xlate**-Objekte in eine globale Adresse.

Gehen Sie wie folgt vor, um internen Hosts den Zugriff auf externe Netzwerke mit PAT zu ermöglichen:

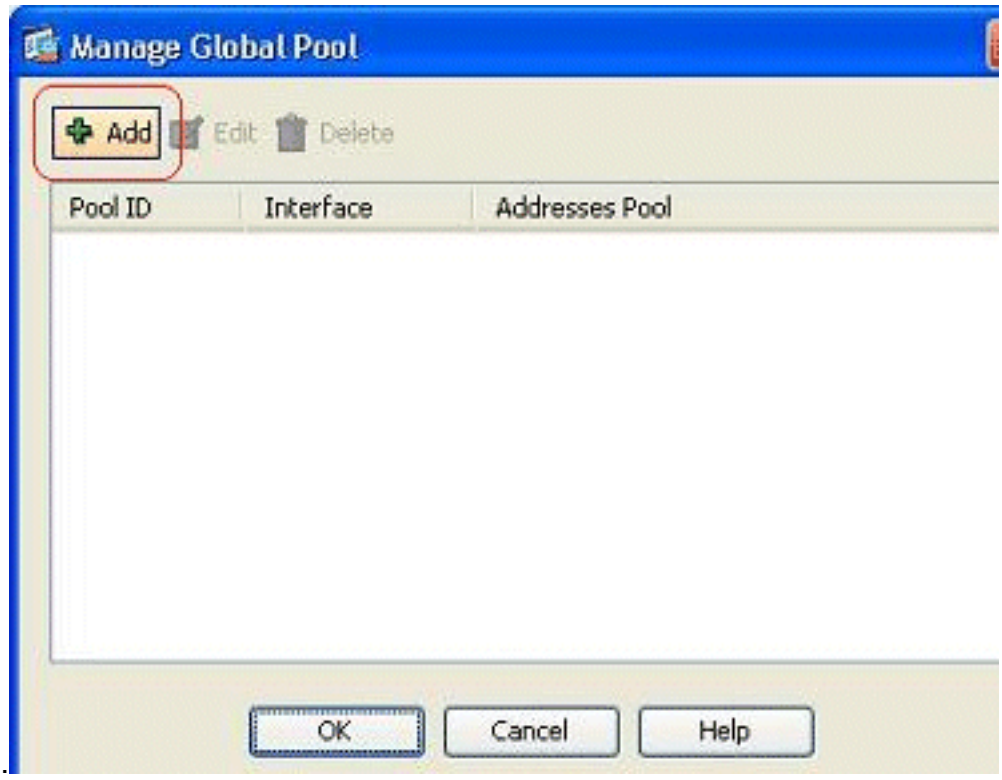
1. Gehen Sie zu **Konfiguration > Firewall > NAT Rules**, klicken Sie auf **Hinzufügen**, und wählen Sie dann die **Option Dynamische NAT-Regel hinzufügen aus, um eine dynamische NAT-Regel zu konfigurieren.**



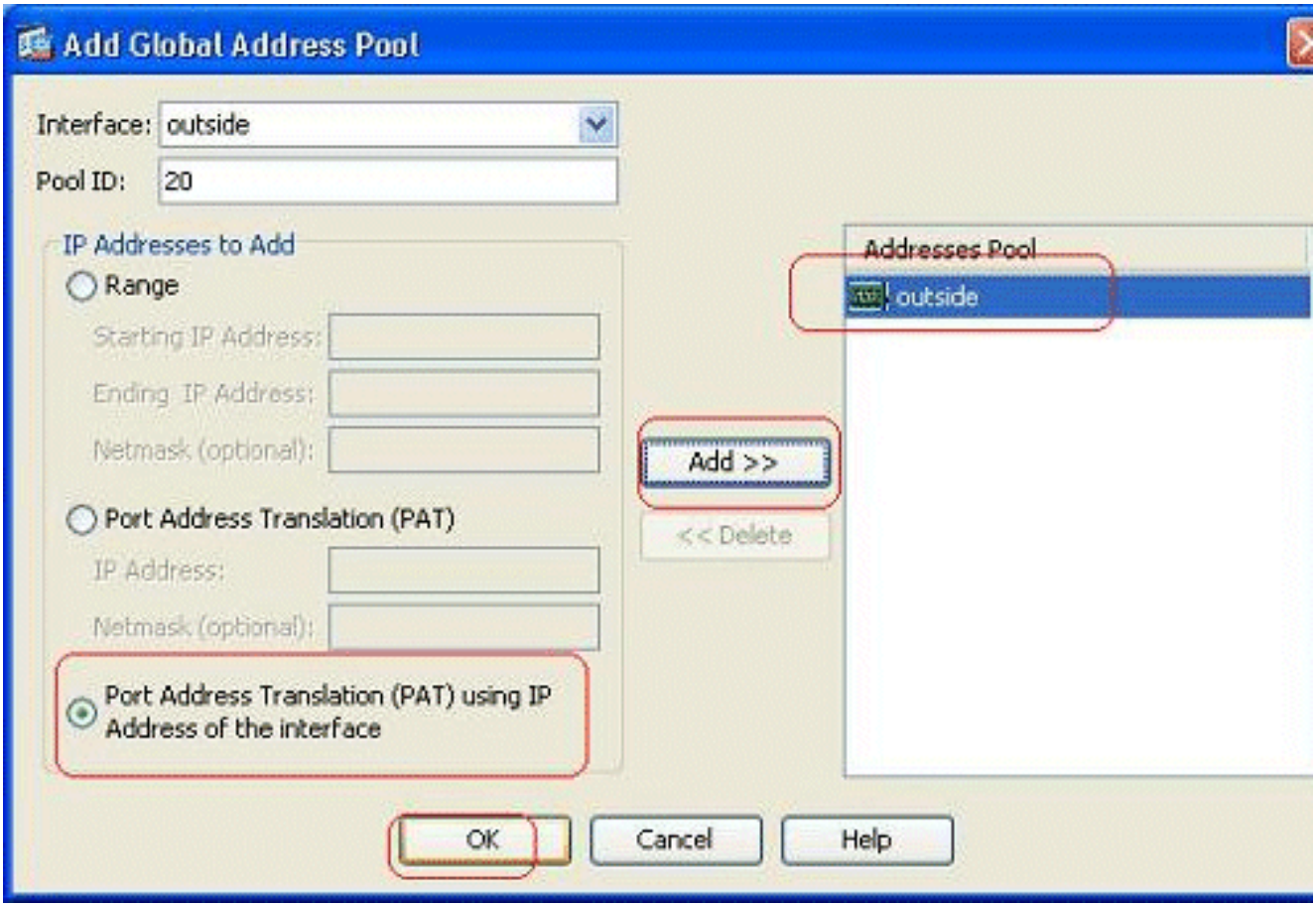
2. Wählen Sie den Namen der Schnittstelle aus, mit der die echten Hosts verbunden sind. Wählen Sie die tatsächliche IP-Adresse der Hosts/Netzwerke mithilfe der Schaltfläche **Details** im Feld **Source (Quelle) aus**, und wählen Sie **inside network (Netzwerkintern)** aus. Klicken Sie auf **Verwalten**, um die Informationen zur übersetzten Adresse zu definieren.



3. Klicken Sie auf **Hinzufügen**.

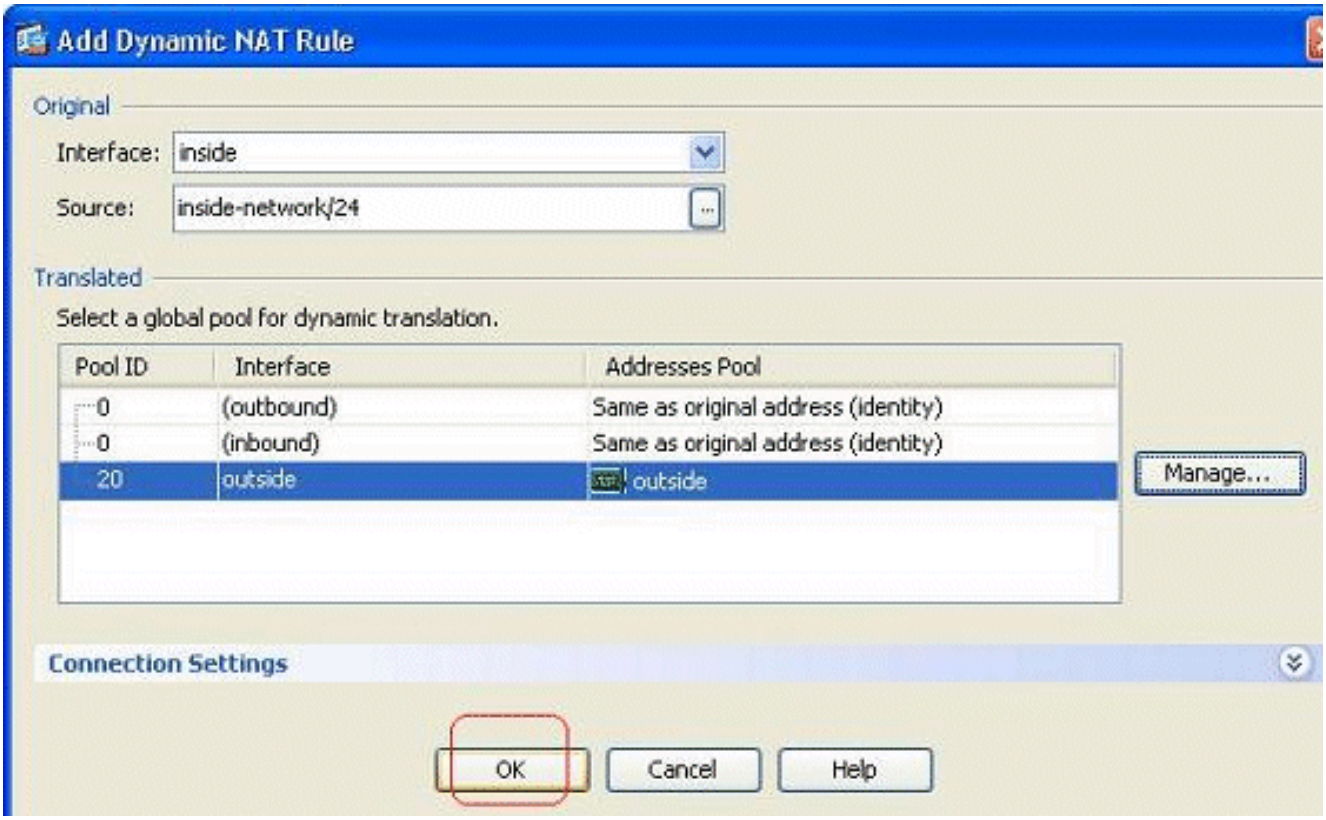


4. Wählen Sie die **Port Address Translation (PAT) mithilfe der IP-Adresse der Schnittstellenoption aus**, und klicken Sie auf **Add**, um sie dem Adresspool hinzuzufügen. Vergessen Sie nicht, eine eindeutige ID für diesen NAT-Adresspool zuzuweisen.

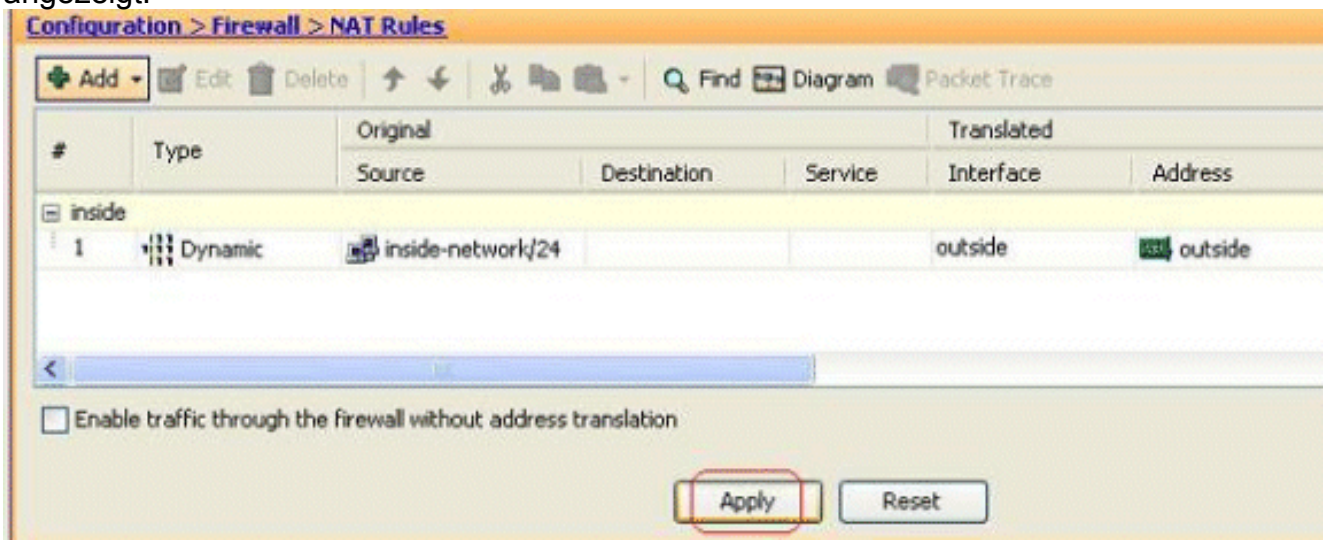


5. Hier sehen Sie den konfigurierten Adresspool mit der externen Schnittstelle als einzige verfügbare Adresse in diesem Pool. Klicken Sie auf **OK**, um zum Fenster Dynamische NAT-Regel hinzufügen zurückzukehren.

6. Klicken Sie auf **OK**.



7. Die konfigurierte dynamische NAT-Regel wird hier im Bereich Konfiguration > Firewall > NAT Rules (Konfiguration > Firewall > NAT-Regeln) angezeigt.



Dies ist die entsprechende CLI-Ausgabe für diese PAT-Konfiguration:

```
global (outside) 20 interface
nat (inside) 20 172.16.11.0 255.255.255.0
```

Einschränken des Zugriffs von internen Hosts auf externe Netzwerke

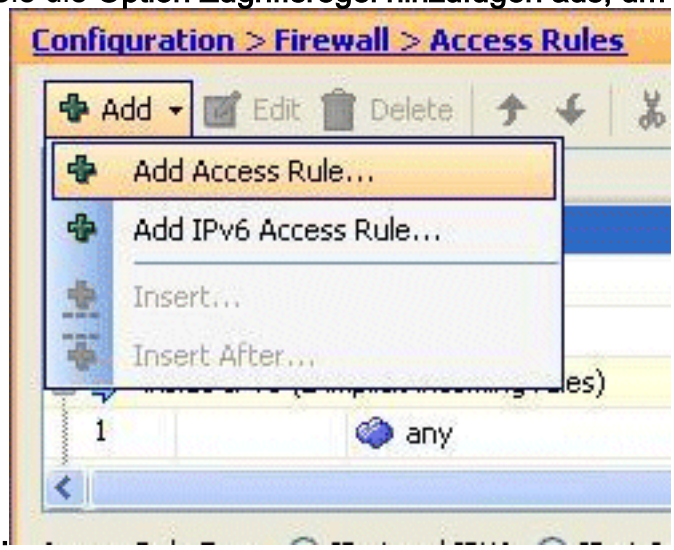
Wenn keine Zugriffsregeln definiert sind, können Benutzer über eine Schnittstelle mit höherer Sicherheit auf alle Ressourcen zugreifen, die einer Schnittstelle mit niedrigerer Sicherheit zugeordnet sind. Um den Zugriff bestimmter Benutzer auf bestimmte Ressourcen zu beschränken, verwenden Sie die Zugriffsregeln im ASDM. In diesem Beispiel wird beschrieben, wie ein einzelner Benutzer auf externe Ressourcen (über FTP, SMTP, POP3, HTTPS und WWW)

zugreifen und alle anderen daran hindern kann, auf externe Ressourcen zuzugreifen.

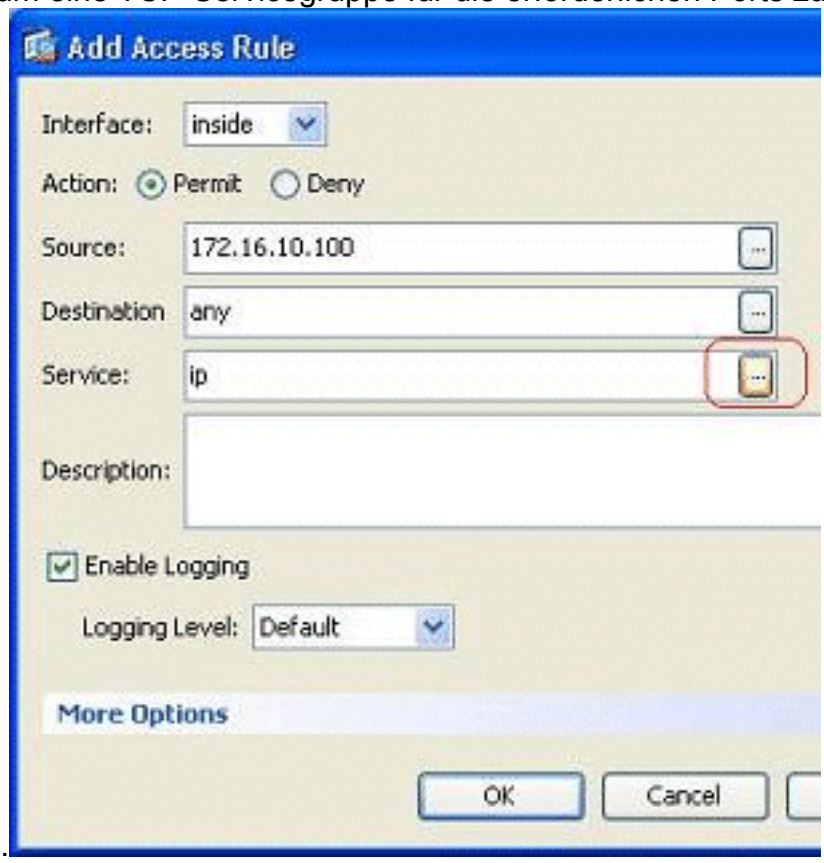
Hinweis: Am Ende jeder Zugriffsliste gibt es eine "Implicit Deny"-Regel.

Gehen Sie wie folgt vor:

1. Gehen Sie zu **Konfiguration > Firewall > Zugriffsregeln**, klicken Sie auf **Hinzufügen**, und wählen Sie die **Option Zugriffsregel hinzufügen aus, um einen neuen Zugriffslisteneintrag zu erstellen.**

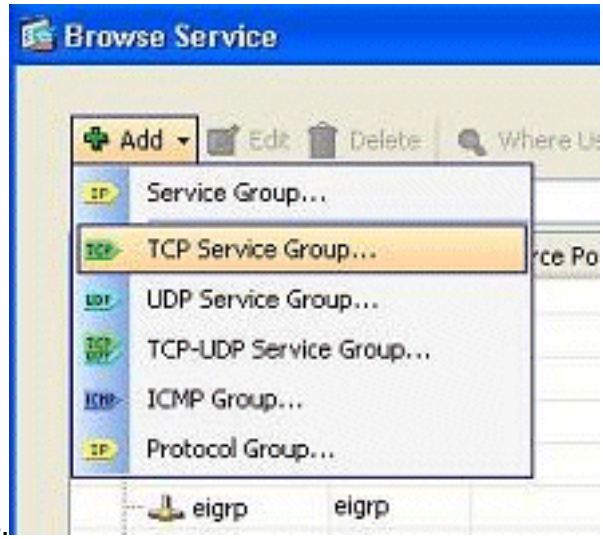


2. Wählen Sie die Quell-IP-Adresse aus, die im Feld **Source (Quelle)** zugelassen werden soll. Wählen Sie **any** als Destination (Ziel), **inside** als Interface (Schnittstelle) und **Permit (Zulassen)** als Action aus. Klicken Sie schließlich im Feld Service auf die Schaltfläche **Details**, um eine TCP-Servicegruppe für die erforderlichen Ports zu erstellen.

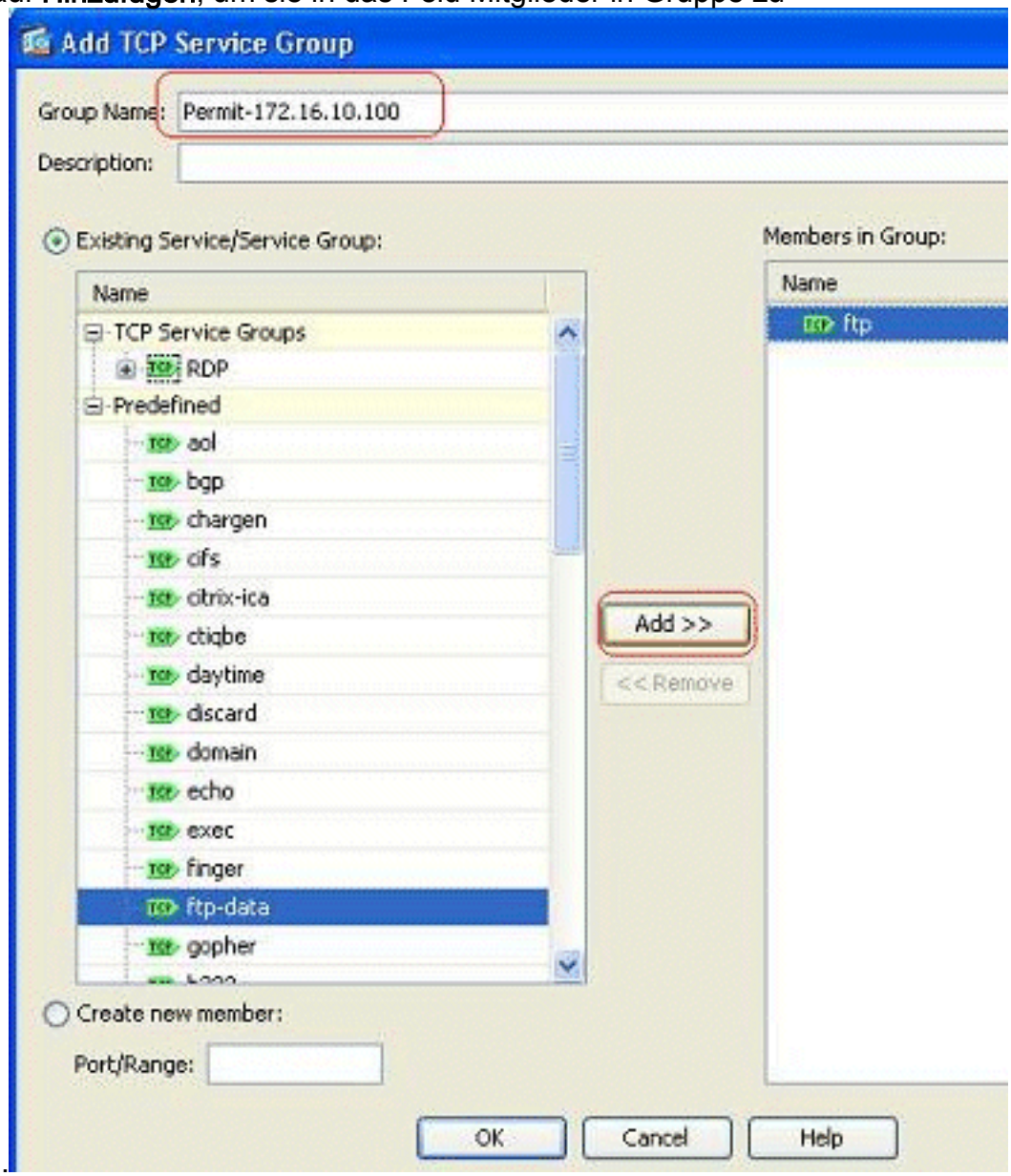


3. Klicken Sie auf **Hinzufügen**, und wählen Sie dann die Option **TCP Service Group (TCP-**

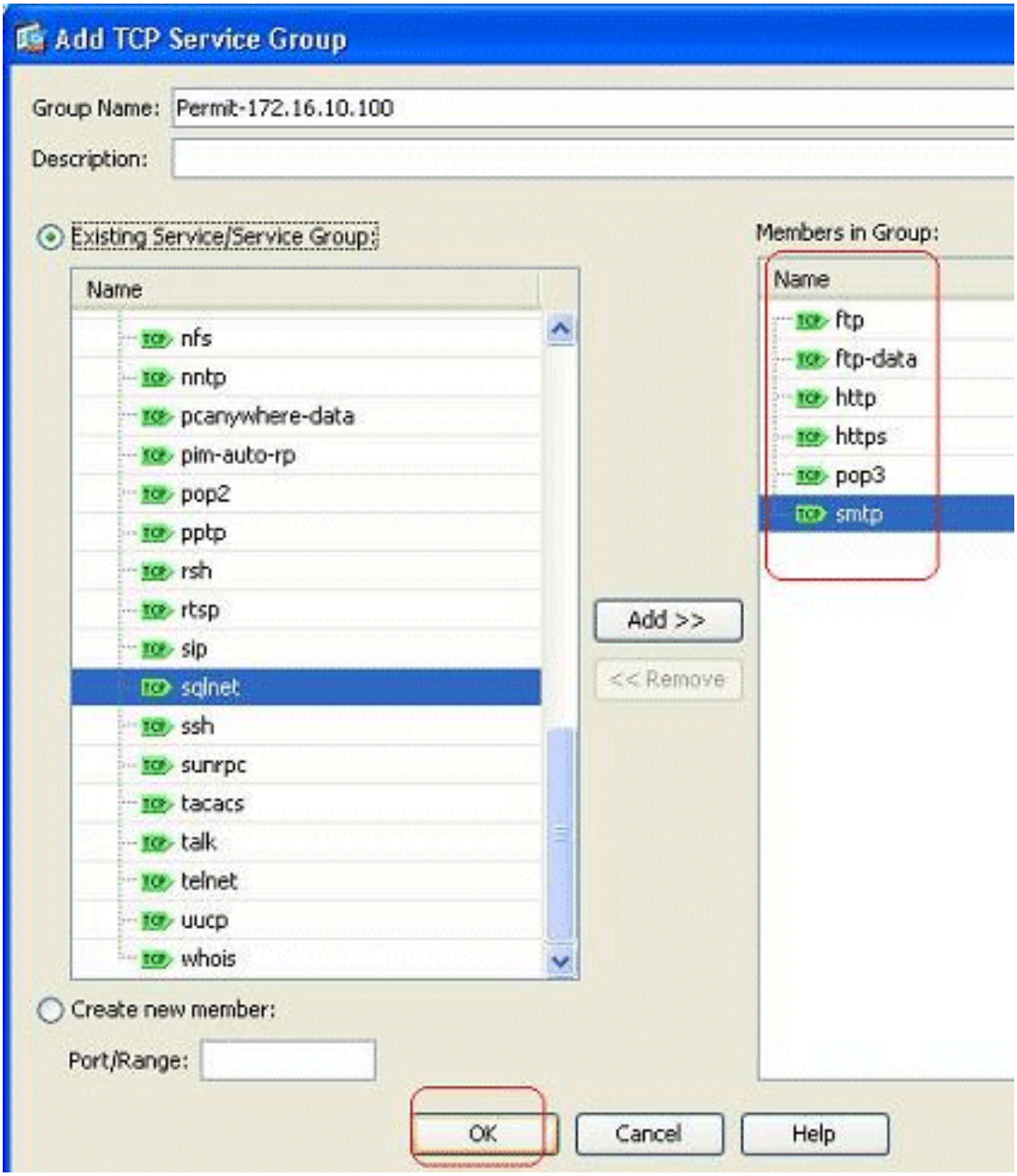
Servicegruppe) aus.



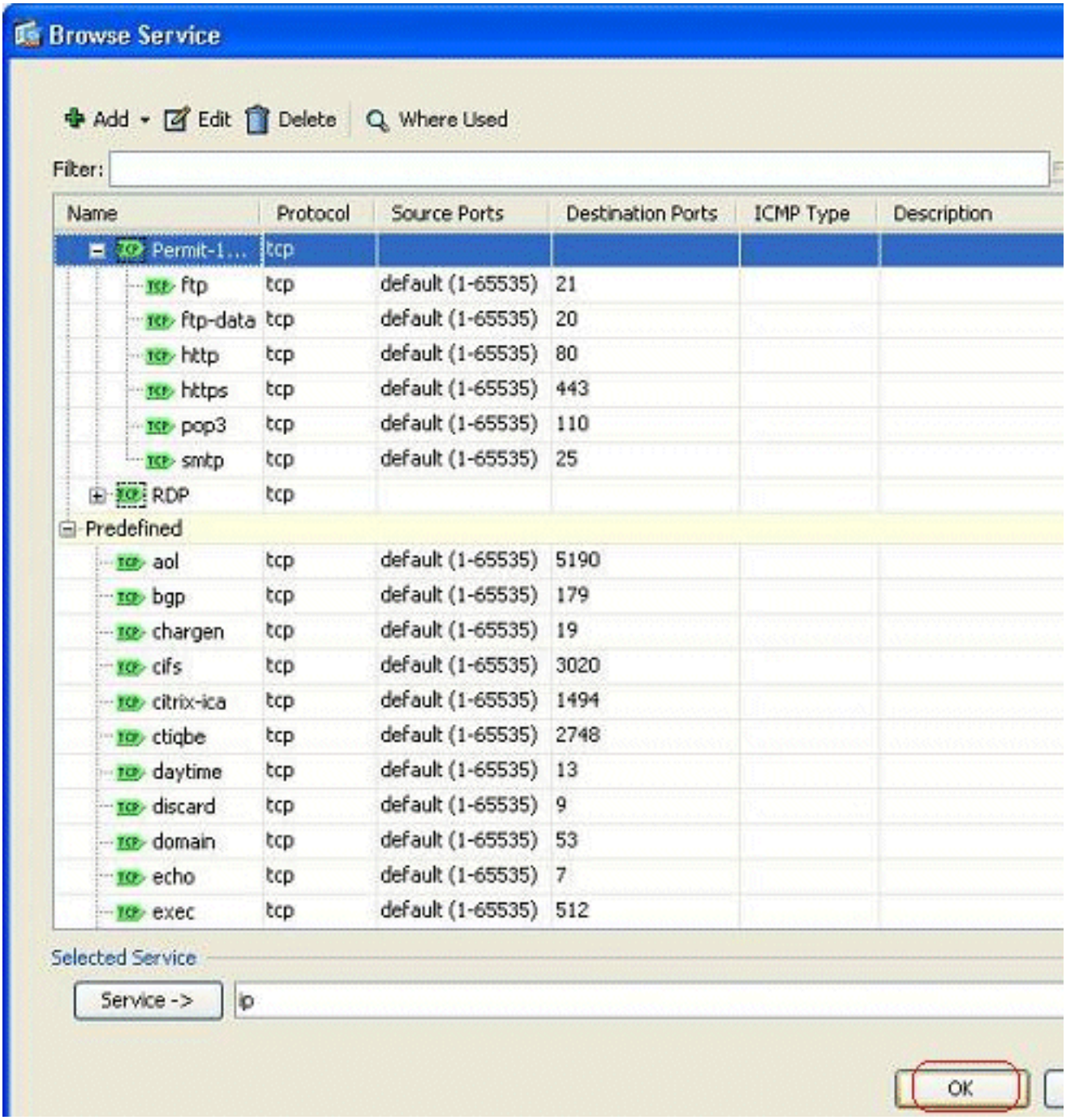
4. Geben Sie einen Namen für diese Gruppe ein. Wählen Sie alle erforderlichen Ports aus, und klicken Sie auf **Hinzufügen**, um sie in das Feld Mitglieder in Gruppe zu verschieben.



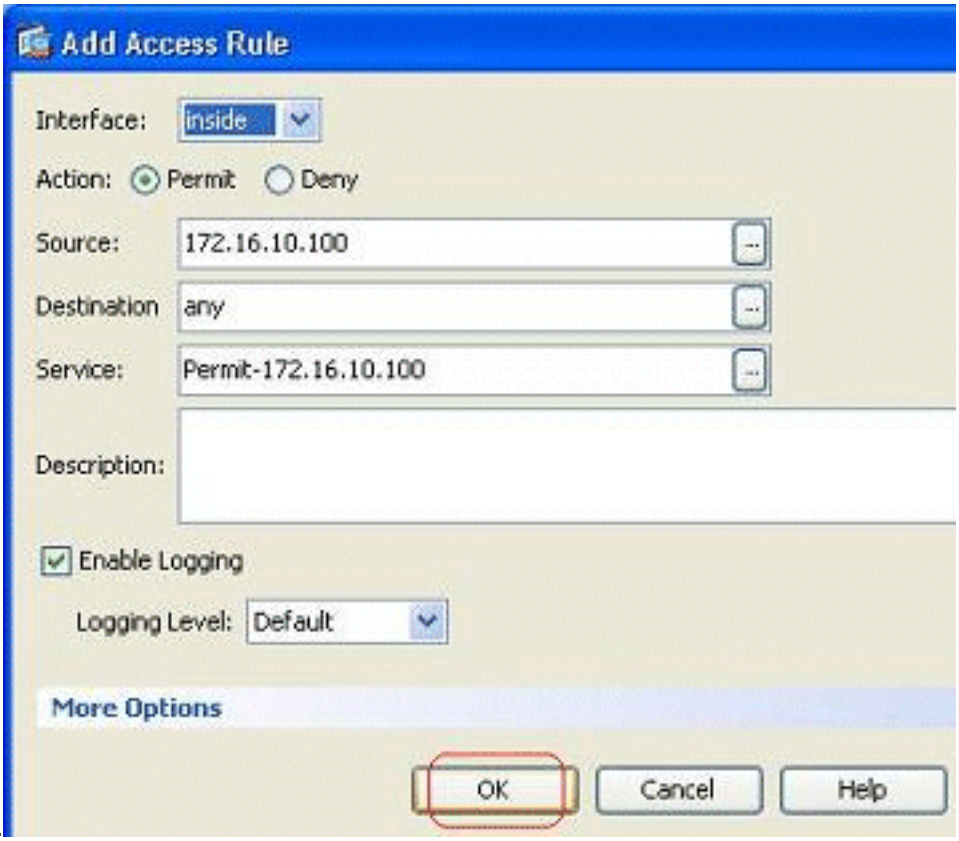
5. Alle ausgewählten Ports sollten im rechten Feld angezeigt werden. Klicken Sie auf **OK**, um die Auswahl der Service-Ports abzuschließen.



6. Hier sehen Sie die konfigurierte TCP-Servicegruppe. Klicken Sie auf **OK**.

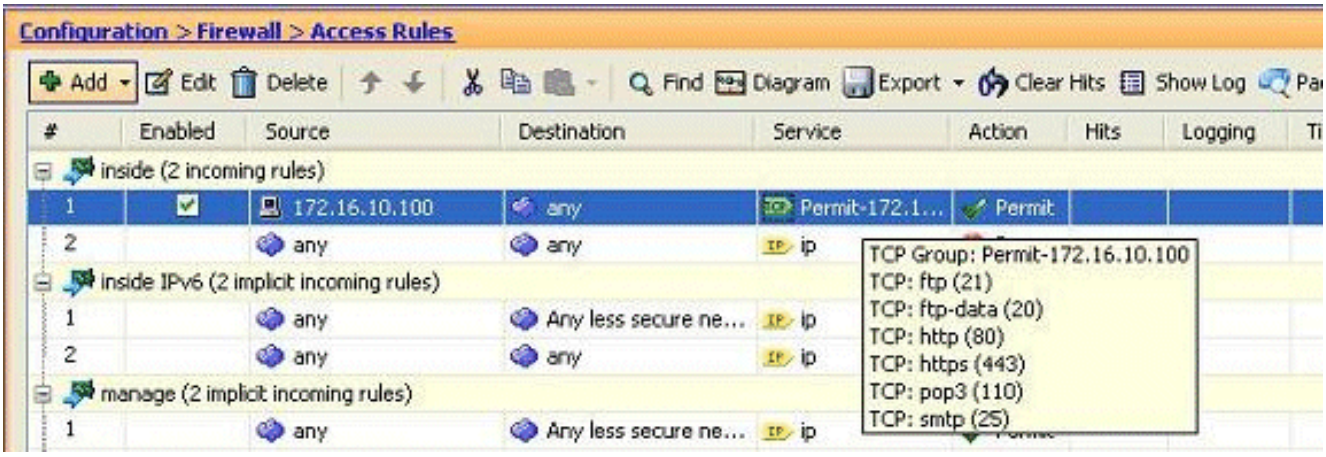


7. Klicken Sie auf **OK**, um die Konfiguration

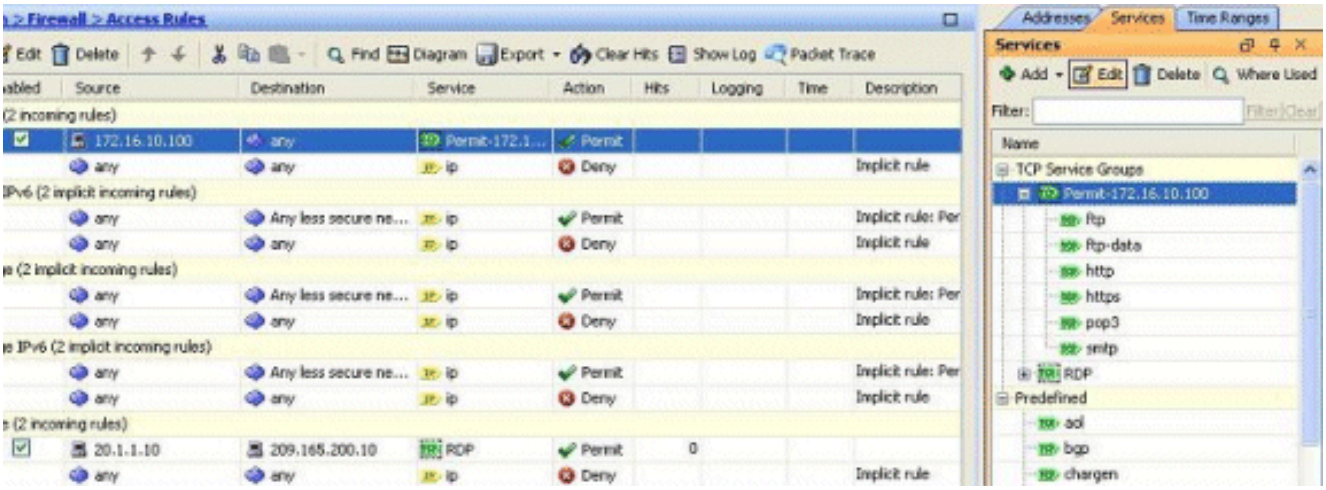


abzuschließen.

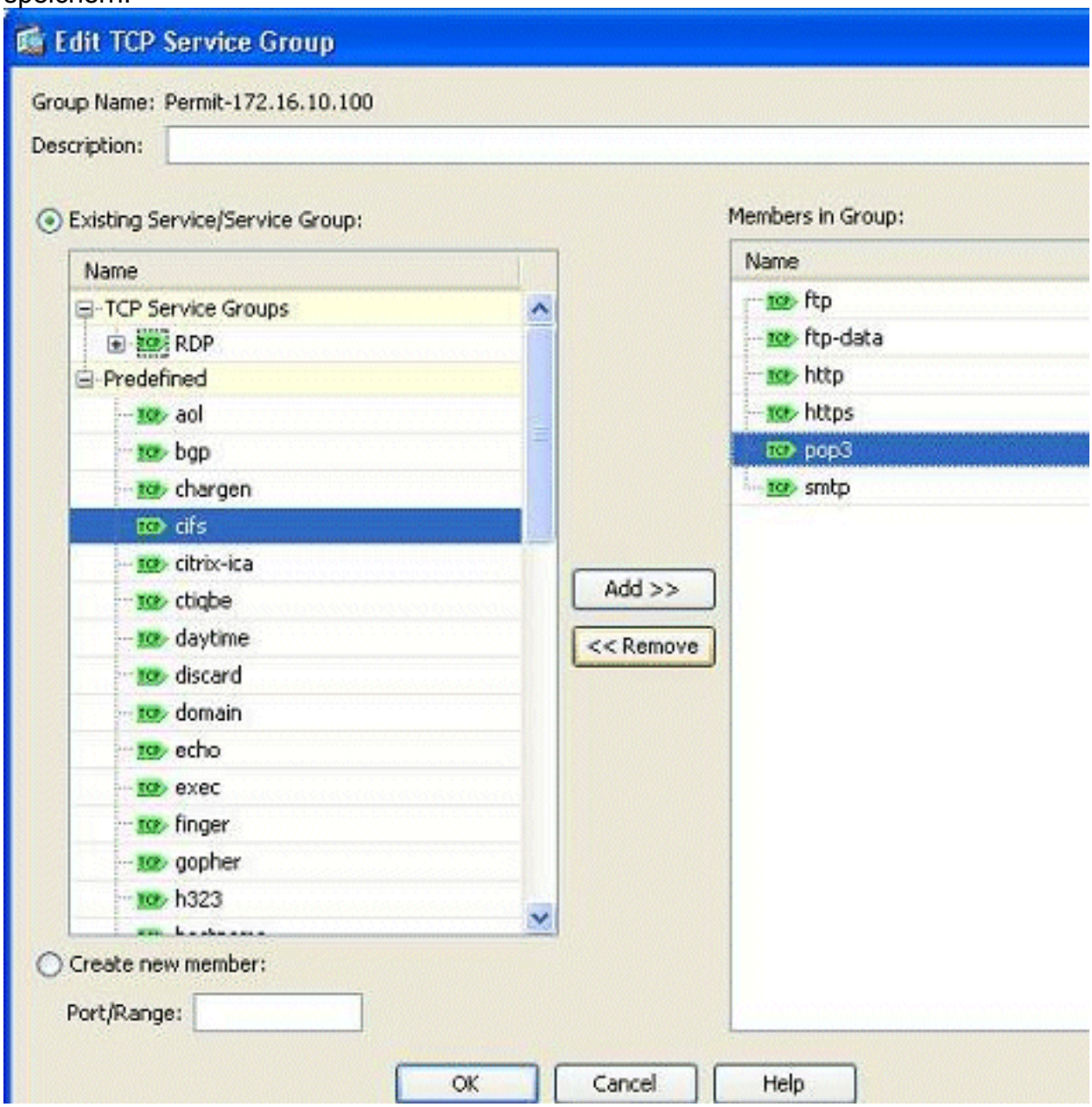
8. Die konfigurierte Zugriffsregel ist unter der **internen** Schnittstelle im Bereich Konfiguration > Firewall > Zugriffsregeln
sichtbar.



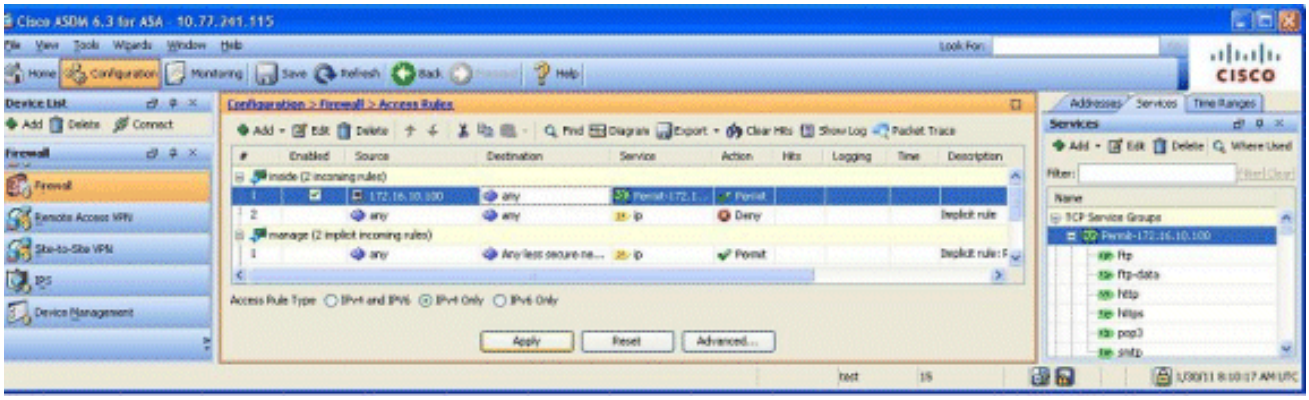
9. Um die Verwendung zu vereinfachen, können Sie die TCP-Service-Gruppe auch direkt im rechten Bereich der Registerkarte **Services** bearbeiten. Klicken Sie auf **Bearbeiten**, um diese Servicegruppe direkt zu
ändern.



10. Sie wird erneut zum Fenster "Edit TCP Service Group" (TCP-Servicegruppe bearbeiten) umgeleitet. Nehmen Sie Änderungen entsprechend Ihren Anforderungen vor, und klicken Sie auf **OK**, um die Änderungen zu speichern.



11. Hier sehen Sie eine vollständige Übersicht über das ASDM:



Dies ist die entsprechende CLI-Konfiguration:

```
object-group service Permit-172.16.10.100 TCP
 port-object eq ftp
 port-object eq ftp-data
 port-object eq www
 port-object eq https
 port-object eq pop3
 port-object eq smtp
!
access-list inside_access_in extended permit TCP host 172.16.10.100 any
    object-group Permit-172.16.10.100
!
access-group inside_access_in in interface inside
!
```

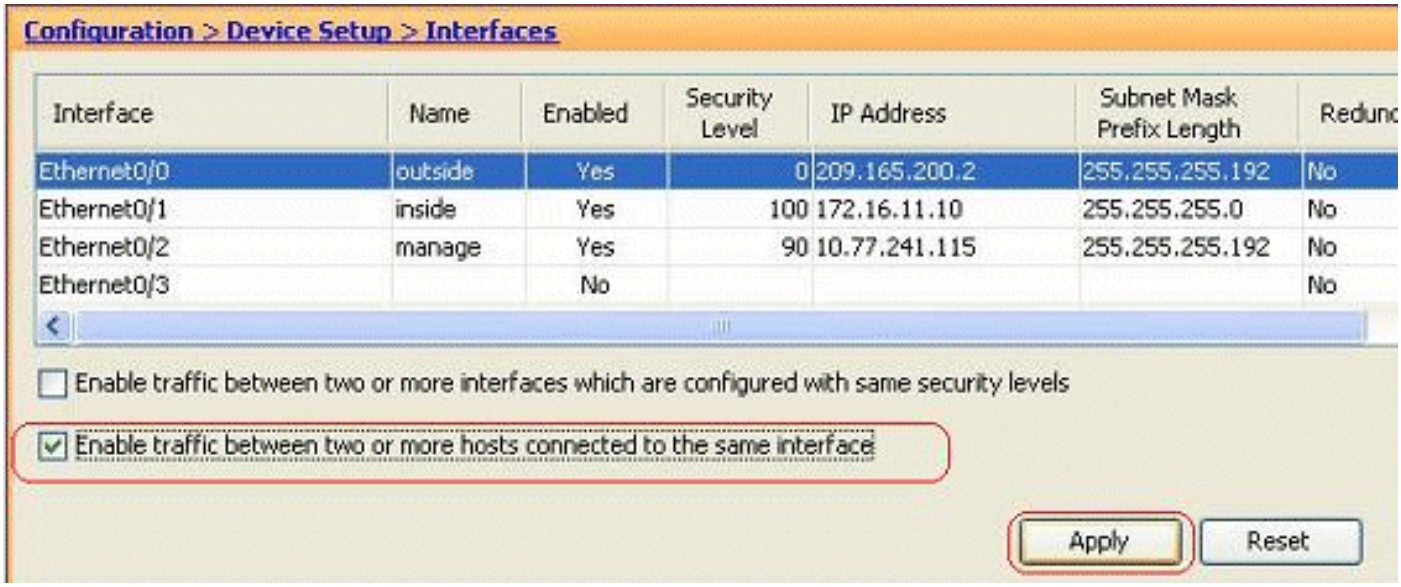
Vollständige Informationen zur Implementierung der Zugriffskontrolle finden Sie unter Hinzufügen oder Ändern einer Zugriffsliste über die ASDM-GUI.

Datenverkehr zwischen Schnittstellen mit derselben Sicherheitsstufe zulassen

In diesem Abschnitt wird beschrieben, wie der Datenverkehr innerhalb von Schnittstellen mit den gleichen Sicherheitsstufen aktiviert wird.

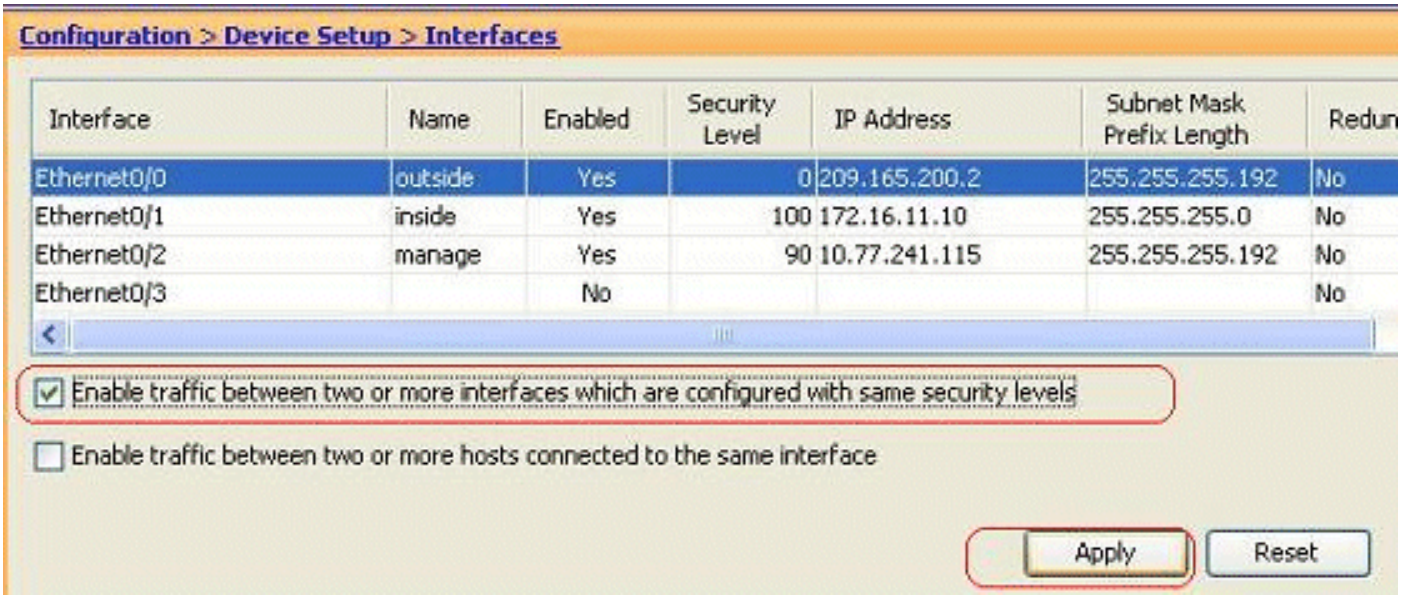
In diesen Anweisungen wird beschrieben, wie die Kommunikation zwischen den Schnittstellen aktiviert wird.

Dies ist für VPN-Datenverkehr hilfreich, der in eine Schnittstelle eingeht, aber dann über dieselbe Schnittstelle weitergeleitet wird. Der VPN-Datenverkehr kann in diesem Fall unverschlüsselt oder für eine andere VPN-Verbindung neu verschlüsselt werden. Gehen Sie zu **Configuration > Device Setup > Interfaces**, und wählen Sie die **Option Enable traffic between two or more hosts connected to the same interface** aus.



In diesen Anweisungen wird beschrieben, wie die Kommunikation zwischen den Schnittstellen aktiviert wird.

Dies ist nützlich, um die Kommunikation zwischen Schnittstellen mit gleichen Sicherheitsstufen zu ermöglichen. Gehen Sie zu **Configuration > Device Setup > Interfaces**, und wählen Sie **Enable traffic between two or more interfaces, which are configured with same security levels** option.



Dies ist die entsprechende CLI für beide Einstellungen:

```
same-security-traffic permit intra-interface
same-security-traffic permit inter-interface
```

Zugriff für nicht vertrauenswürdige Hosts auf Hosts in Ihrem vertrauenswürdigen Netzwerk zulassen

Dies kann durch die Anwendung einer statischen NAT-Übersetzung und einer Zugriffsregel erreicht werden, die diese Hosts zulässt. Sie müssen dies immer konfigurieren, wenn ein externer Benutzer auf einen Server im internen Netzwerk zugreifen möchte. Der Server im internen Netzwerk verfügt über eine private IP-Adresse, die im Internet nicht routbar ist. Daher müssen Sie diese private IP-Adresse mithilfe einer statischen NAT-Regel in eine öffentliche IP-Adresse

übersetzen. Angenommen, Sie haben einen internen Server (172.16.11.5). Damit dies funktioniert, müssen Sie diese private Server-IP in eine öffentliche IP-Adresse übersetzen. In diesem Beispiel wird beschrieben, wie die bidirektionale statische NAT für die Übersetzung von 172.16.11.5 in 209.165.200.5 implementiert wird.

Der Abschnitt, der es externen Benutzern ermöglicht, durch Implementierung einer Zugriffsregel auf diesen Webserver zuzugreifen, wird hier nicht angezeigt. Hier wird ein kurzer CLI-Ausschnitt angezeigt, um Ihnen das Verständnis zu erleichtern:

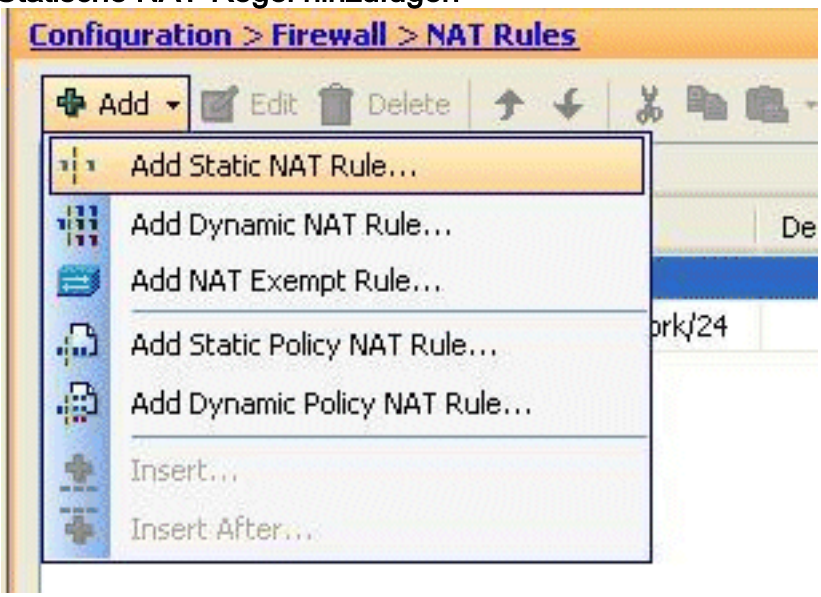
```
access-list 101 permit TCP any host 209.165.200.5
```

Weitere Informationen finden Sie unter Hinzufügen oder Ändern einer Zugriffsliste über die ASDM-GUI.

Hinweis: Durch die Angabe des Schlüsselworts "any" können beliebige Benutzer von außerhalb auf diesen Server zugreifen. Wenn sie für keine Service-Ports angegeben ist, kann der Zugriff auf den Server auf jedem Service-Port erfolgen, wenn diese offen bleiben. Seien Sie vorsichtig, wenn Sie die Implementierung durchführen. Wir empfehlen Ihnen, die Berechtigung auf den einzelnen externen Benutzer und auch auf den erforderlichen Port des Servers zu beschränken.

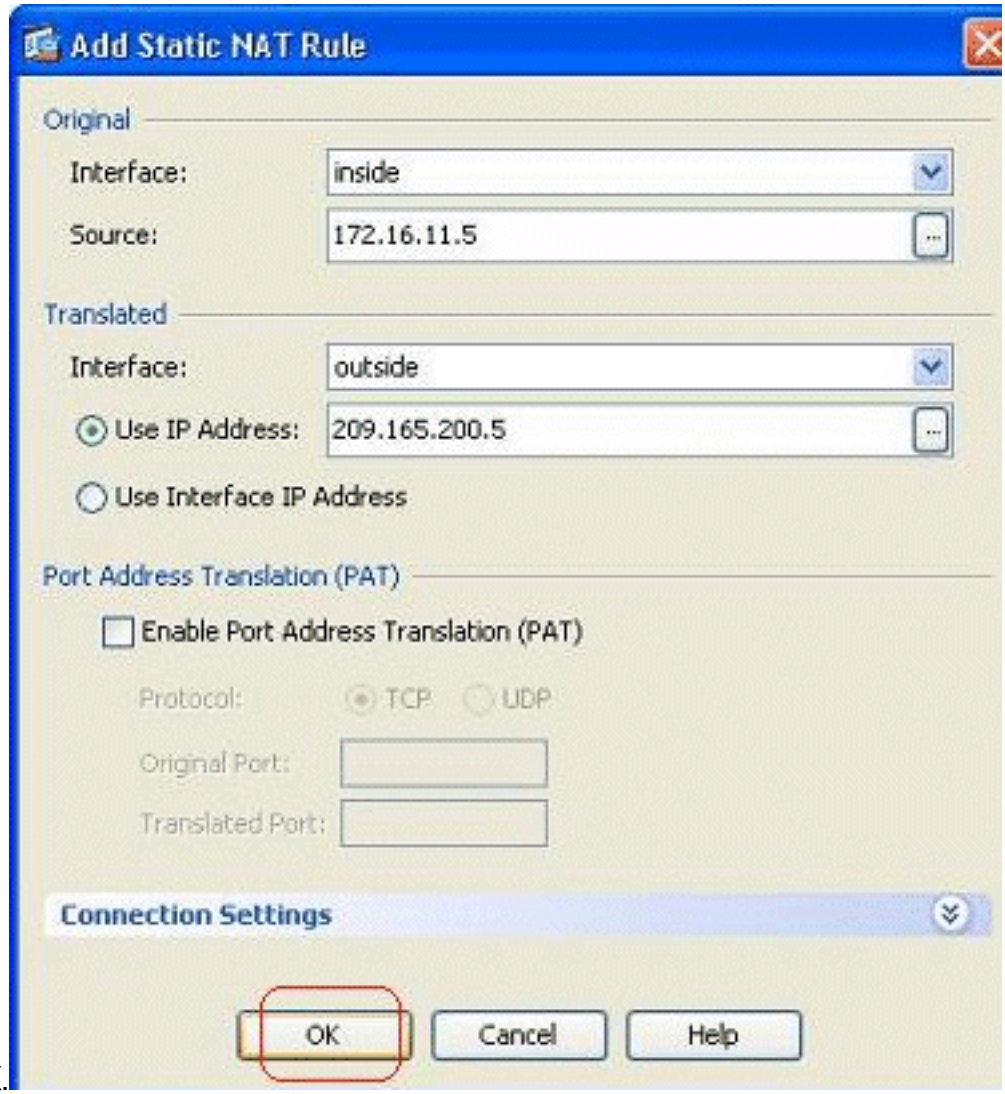
Gehen Sie wie folgt vor, um die statische NAT zu konfigurieren:

1. Gehen Sie zu **Konfiguration > Firewall > NAT Rules**, klicken Sie auf **Hinzufügen**, und wählen Sie **Statische NAT-Regel hinzufügen**



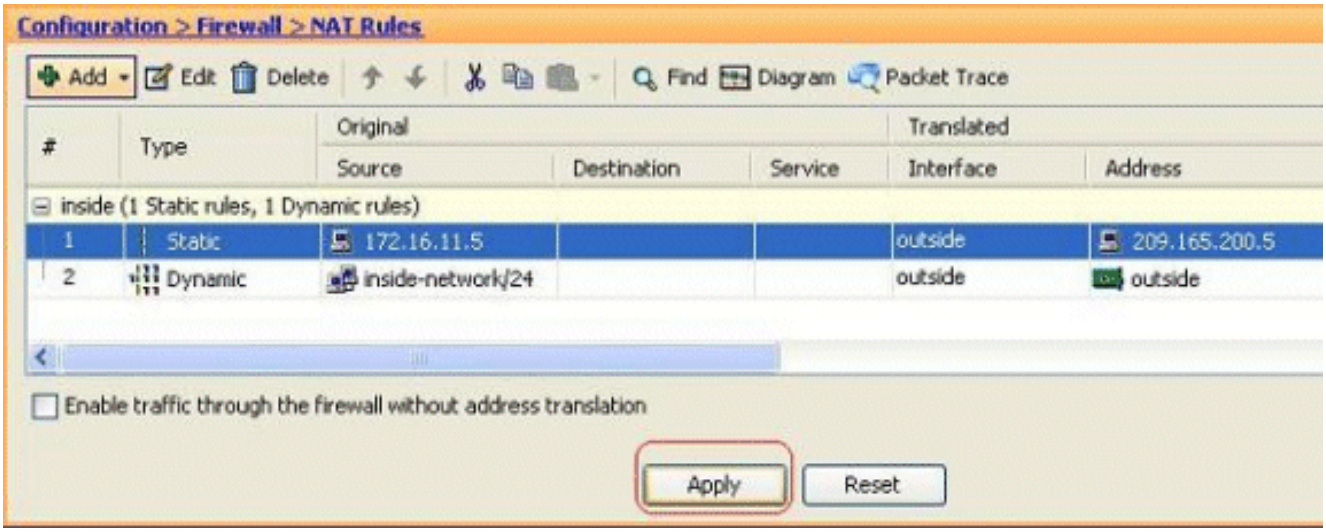
aus.

2. Geben Sie die ursprüngliche IP-Adresse und die übersetzte IP-Adresse zusammen mit den zugehörigen Schnittstellen an, und klicken Sie auf



OK.

3. Hier sehen Sie den konfigurierten statischen NAT-Eintrag. Klicken Sie auf **Apply**, um dies an die ASA zu
senden.



Dies ist ein kurzes CLI-Beispiel für diese ASDM-Konfiguration:

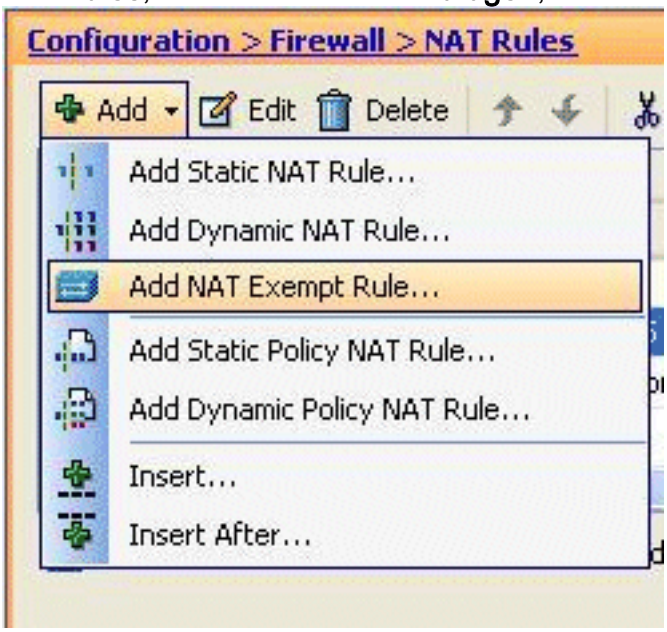
```
!
static (inside,outside) 209.165.200.5 172.16.11.5 netmask 255.255.255.255
!
```

Deaktivieren von NAT für bestimmte Hosts/Netzwerke

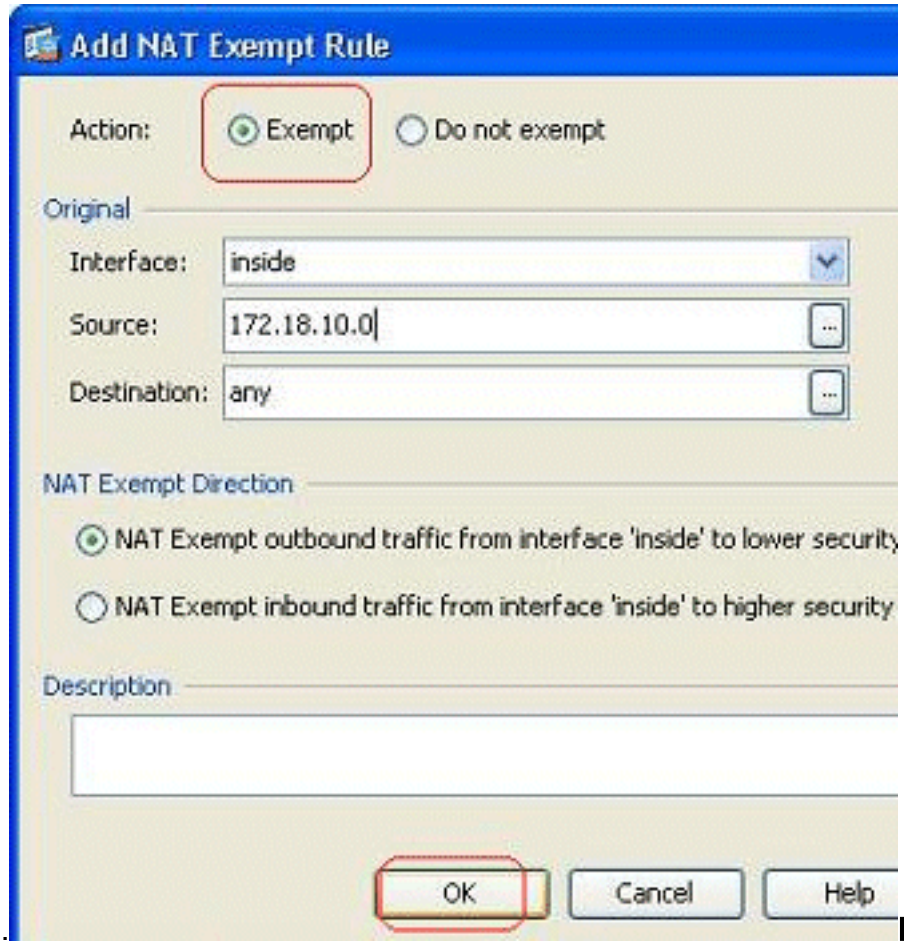
Wenn Sie bestimmte Hosts oder Netzwerke von der NAT ausnehmen müssen, fügen Sie eine NAT-Freistellungsregel hinzu, um die Adressumwandlung zu deaktivieren. Dadurch können sowohl übersetzte als auch Remote-Hosts Verbindungen initiieren.

Gehen Sie wie folgt vor:

1. Gehen Sie zu **Konfiguration > Firewall > NAT Rules**, klicken Sie auf **Hinzufügen**, und wählen Sie **NAT-Befreiungsregel hinzufügen aus.**

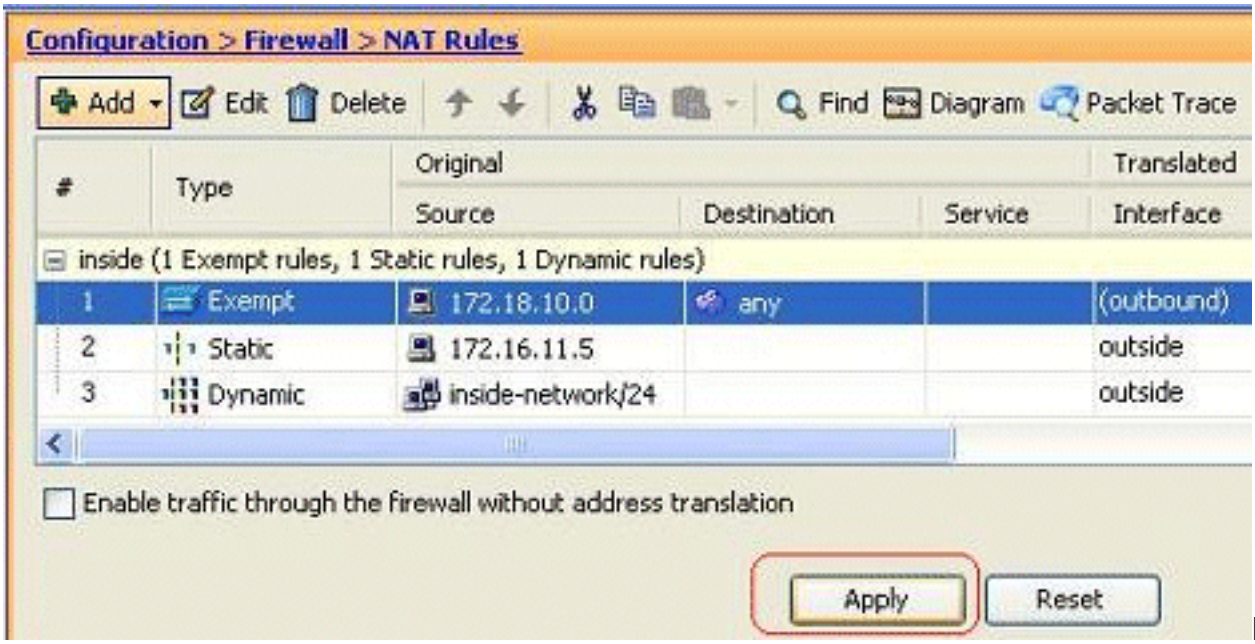


2. Hier wurde das interne Netzwerk 172.18.10.0 von der Adressumwandlung ausgenommen. Vergewissern Sie sich, dass die Option **Exempt** aktiviert wurde. NAT Exempt Direction hat zwei Optionen:Ausgehender Datenverkehr an niedrigere SicherheitsschnittstellenEingehender Datenverkehr an Schnittstellen mit höherer SicherheitDie Standardoption ist für den ausgehenden Datenverkehr. Klicken Sie auf **OK**, um den Schritt



abzuschließen. **Hinweis:** Wenn Sie die Option **Nicht ausnehmen** auswählen, wird dieser Host nicht von NAT ausgenommen, und es wird eine separate Zugriffsregel mit dem Schlüsselwort "Verweigern" hinzugefügt. Dies ist hilfreich, um zu verhindern, dass bestimmte Hosts von NAT ausgenommen werden, da das gesamte Subnetz mit Ausnahme dieser Hosts von der NAT ausgenommen wird.

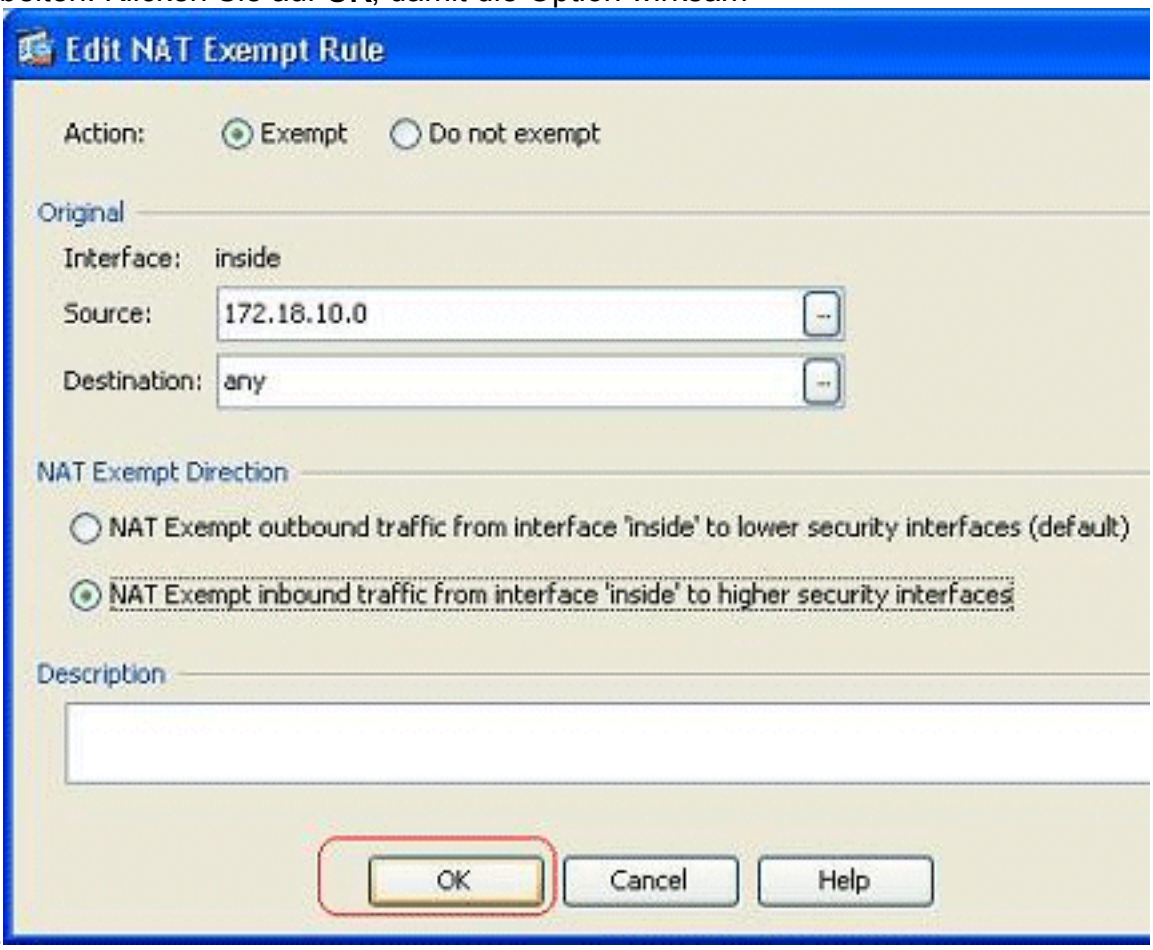
3. Hier sehen Sie die NAT-Ausschlussregel für die ausgehende Richtung. Klicken Sie auf **Apply**, um die Konfiguration an die ASA zu senden.



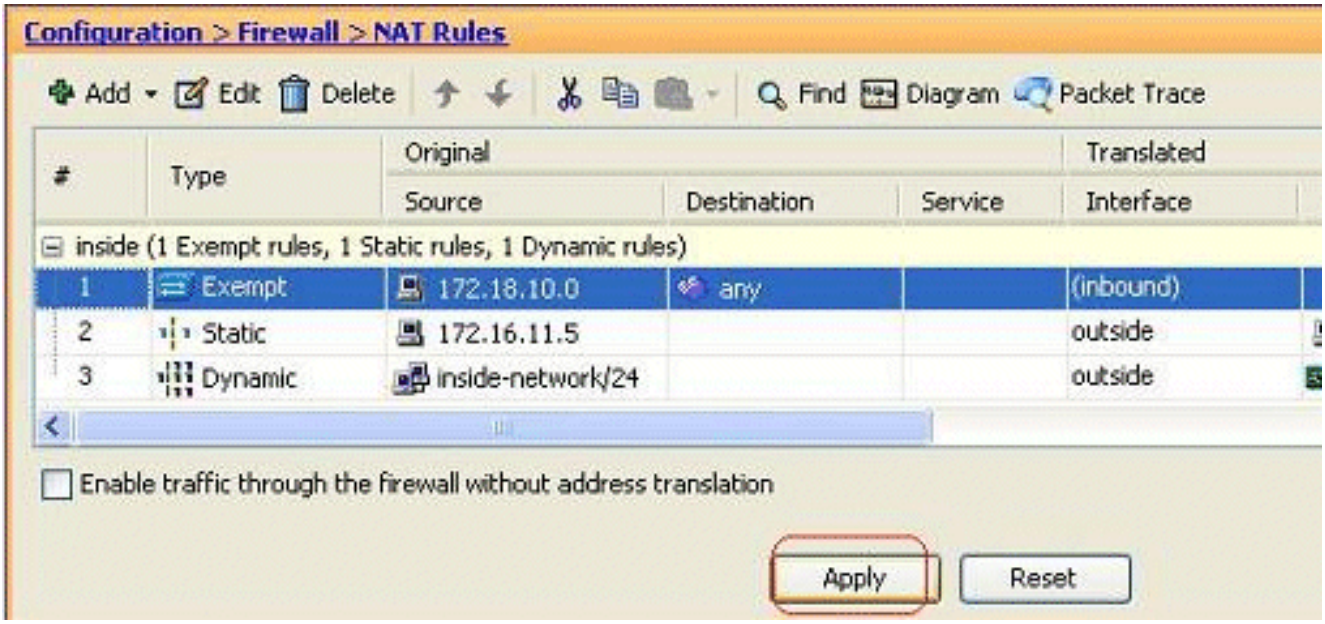
Dies ist die entsprechende CLI-Ausgabe für Ihre Referenz:

```
access-list inside_nat0_outbound extended permit ip host 172.18.10.0 any
!
nat (inside) 0 access-list inside_nat0_outbound
```

4. Hier sehen Sie, wie Sie die NAT-Ausschlussregel für die entsprechende Richtung bearbeiten. Klicken Sie auf **OK**, damit die Option wirksam wird.



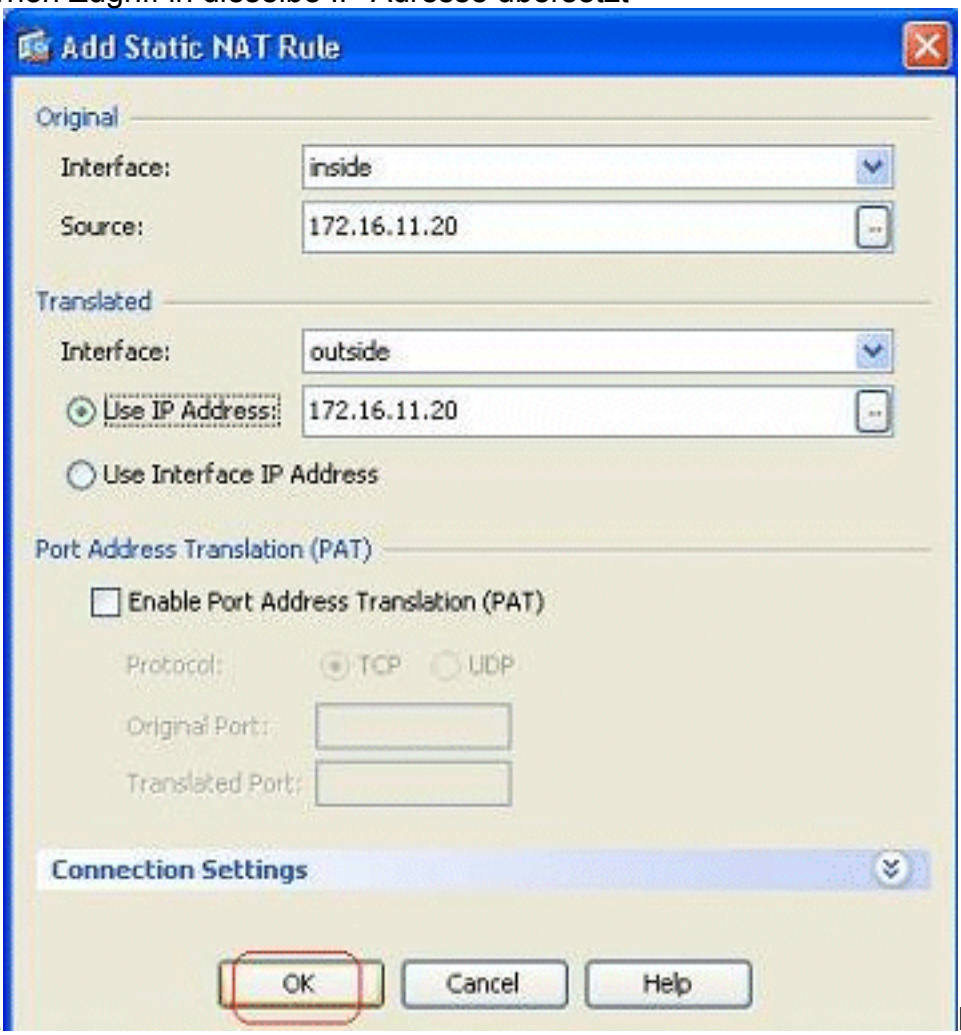
5. Sie können jetzt sehen, dass die Richtung in *eingehend* geändert wurde.



Klicken Sie auf **Apply**, um diese CLI-Ausgabe an die ASA zu senden:

```
access-list inside_nat0_outbound extended permit ip host 172.18.10.0 any
!
nat (inside) 0 access-list inside_nat0_outbound outside
```

Hinweis: Aus diesem Grund sehen Sie, dass am Ende des Befehls **nat 0** ein neues Schlüsselwort (außerhalb) hinzugefügt wurde. Diese Funktion wird als **Outside NAT** bezeichnet.

6. NAT kann auch durch die Implementierung von Identity NAT deaktiviert werden. Identity NAT übersetzt einen Host in dieselbe IP-Adresse. Im folgenden Beispiel wird die NAT für die reguläre statische Identität veranschaulicht, bei der der Host (172.16.11.20) bei einem externen Zugriff in dieselbe IP-Adresse übersetzt wird. 

Dies ist die entsprechende CLI-Ausgabe:

```
!
static (inside,outside) 172.16.11.20 172.16.11.20 netmask 255.255.255.255
!
```

Port Redirection (Forwarding) mit Statics

Port Forwarding oder Port Redirection ist eine nützliche Funktion, bei der externe Benutzer versuchen, auf einen internen Server an einem bestimmten Port zuzugreifen. Um dies zu erreichen, wird der interne Server, der über eine private IP-Adresse verfügt, in eine öffentliche IP-Adresse übersetzt, die wiederum Zugriff für den jeweiligen Port erlaubt.

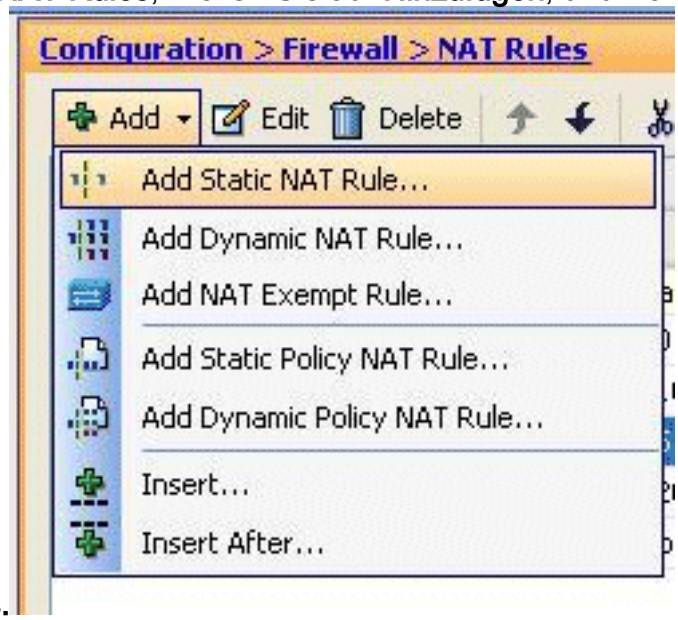
In diesem Beispiel möchte der externe Benutzer auf den SMTP-Server 209.165.200.15 an Port 25 zugreifen. Dies erfolgt in zwei Schritten:

1. Übersetzen Sie den internen Mailserver 172.16.11.15 an Port 25 in die öffentliche IP-Adresse 209.165.200.15 an Port 25.
2. Zugriff auf den öffentlichen Mail-Server 209.165.200.15 an Port 25 zulassen.

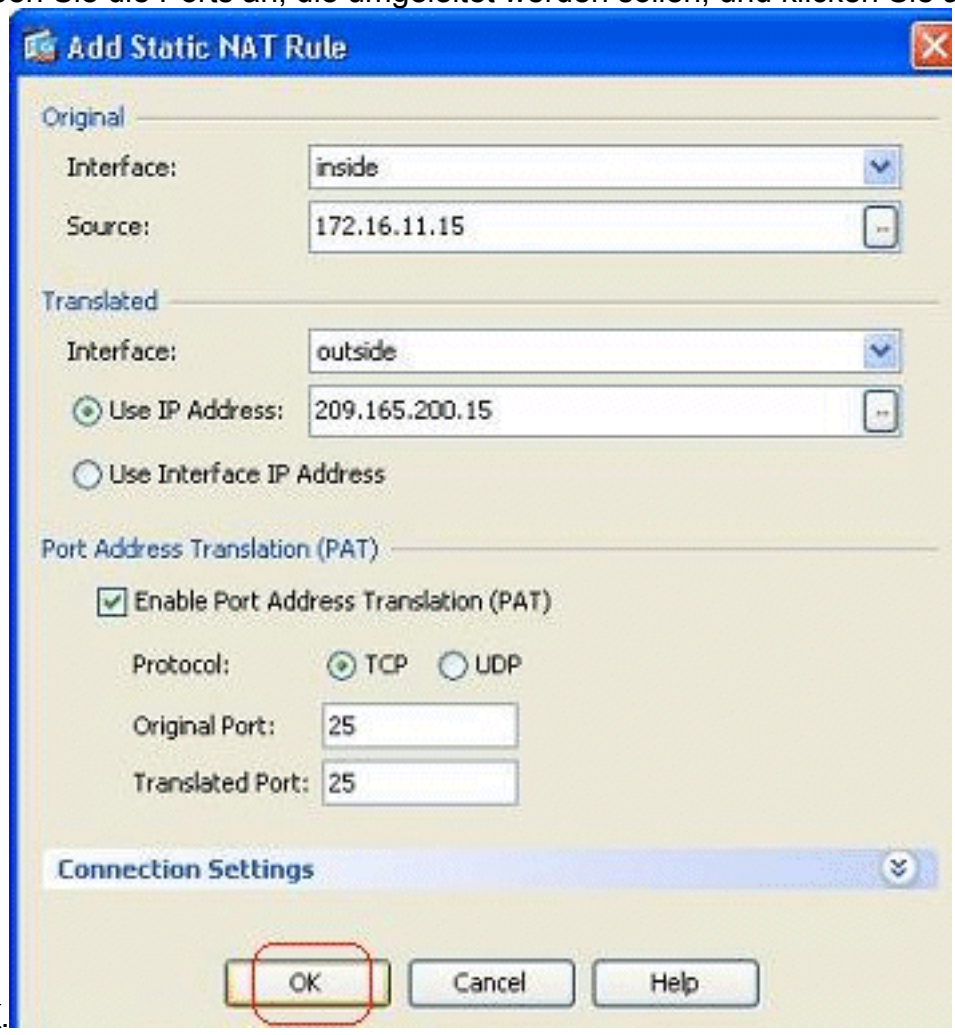
Wenn der externe Benutzer versucht, an Port 25 auf den Server 209.165.200.15 zuzugreifen, wird

dieser Datenverkehr an den internen Mailserver 172.16.11 15 an Port 25 umgeleitet.

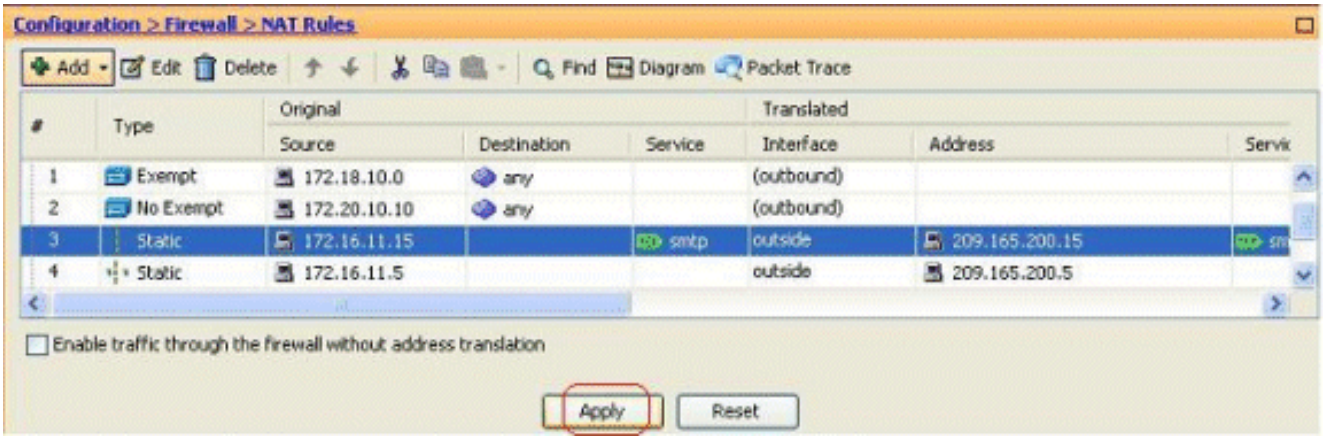
1. Gehen Sie zu **Konfiguration > Firewall > NAT Rules**, klicken Sie auf **Hinzufügen**, und wählen Sie **Statische NAT-Regel hinzufügen aus.**



2. Geben Sie die ursprüngliche Quelle und die übersetzte IP-Adresse zusammen mit den zugehörigen Schnittstellen an. Wählen Sie **Enable Port Address Translation (PAT aktivieren)**, geben Sie die Ports an, die umgeleitet werden sollen, und klicken Sie auf **OK**.



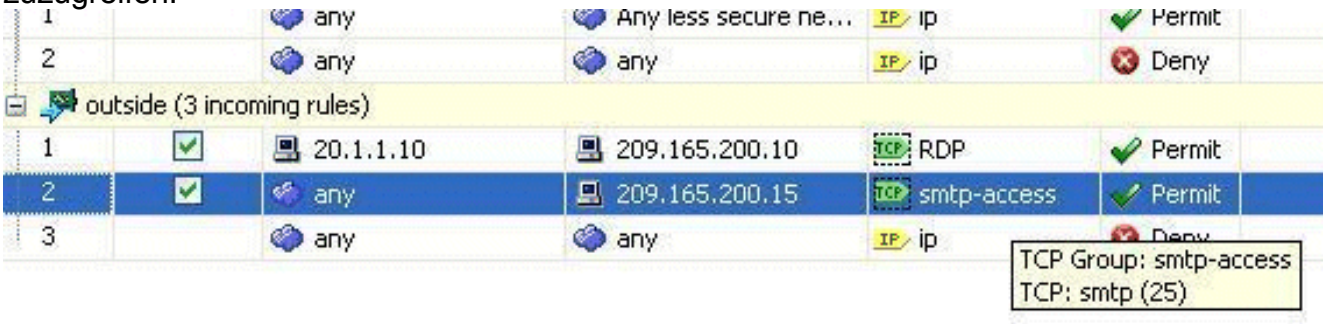
3. Die konfigurierte statische PAT-Regel wird hier angezeigt:



Dies ist die entsprechende CLI-Ausgabe:

```
!
static (inside,outside) TCP 209.165.200.15 smtp 172.16.11.15 smtp netmask
    255.255.255.255
!
```

4. Dies ist die Zugriffsregel, die es externen Benutzern ermöglicht, unter 209.165.200.15 auf den öffentlichen SMTP-Server zuzugreifen:



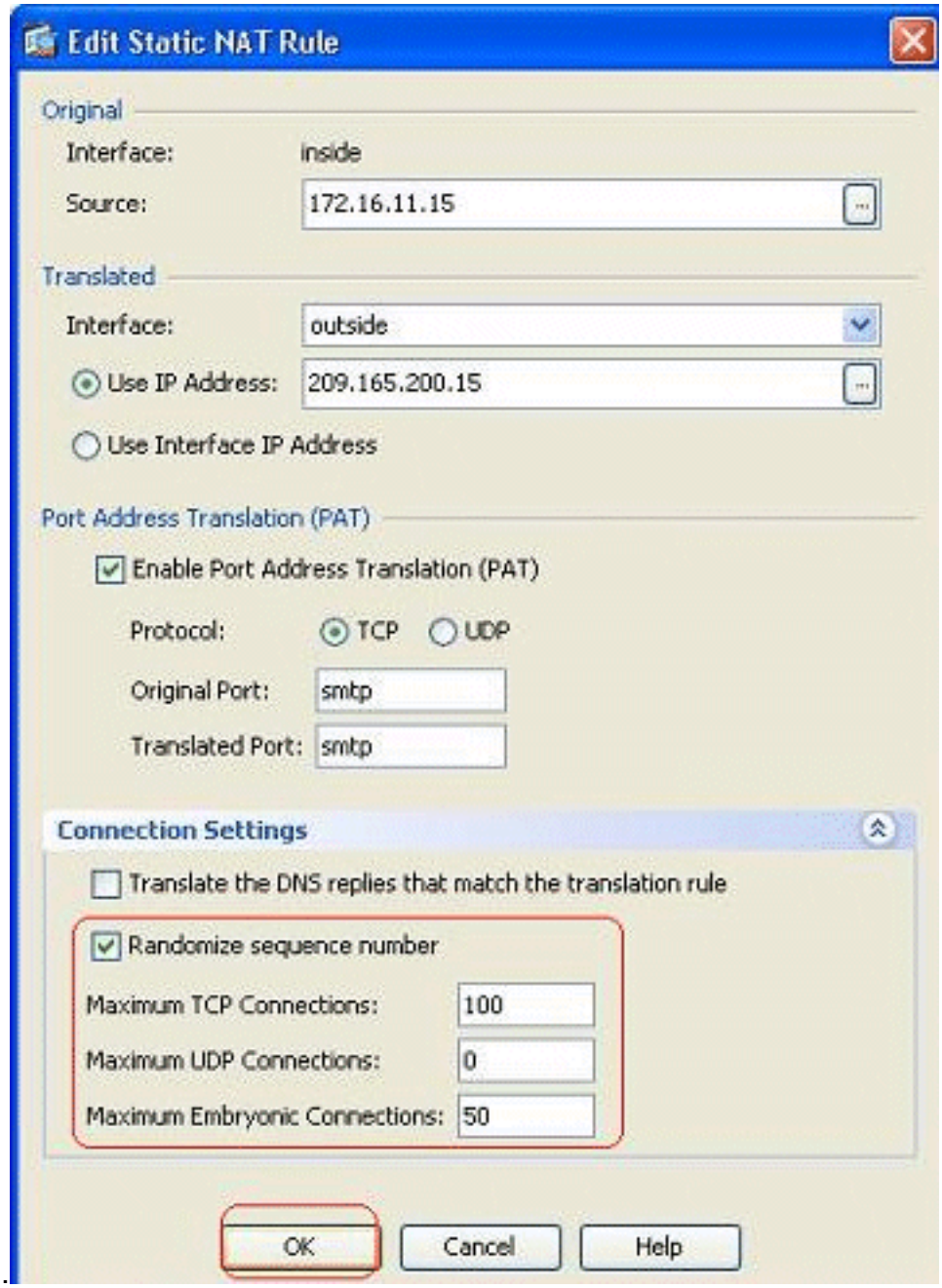
Hinweis: Stellen Sie sicher, dass Sie bestimmte Hosts verwenden, anstatt das **any**-Schlüsselwort in der Quelle der Zugriffsregel zu verwenden.

Begrenzen Sie die TCP/UDP-Sitzung mithilfe von statisch.

Sie können die maximale Anzahl an TCP-/UDP-Verbindungen mithilfe der statischen Regel angeben. Sie können auch die maximale Anzahl an embryonalen Verbindungen angeben. Eine embryonale Verbindung ist eine Verbindung, die halb offen ist. Eine größere Anzahl dieser Aspekte wirkt sich auf die Leistung der ASA aus. Die Einschränkung dieser Verbindungen verhindert bestimmte Angriffe wie DoS und SYN. Um eine vollständige Eindämmung zu erreichen, müssen Sie die Richtlinie im MPF-Framework definieren, das über den Rahmen dieses Dokuments hinausgeht. Weitere Informationen zu diesem Thema finden Sie unter Eindämmen von Netzwerkangriffen.

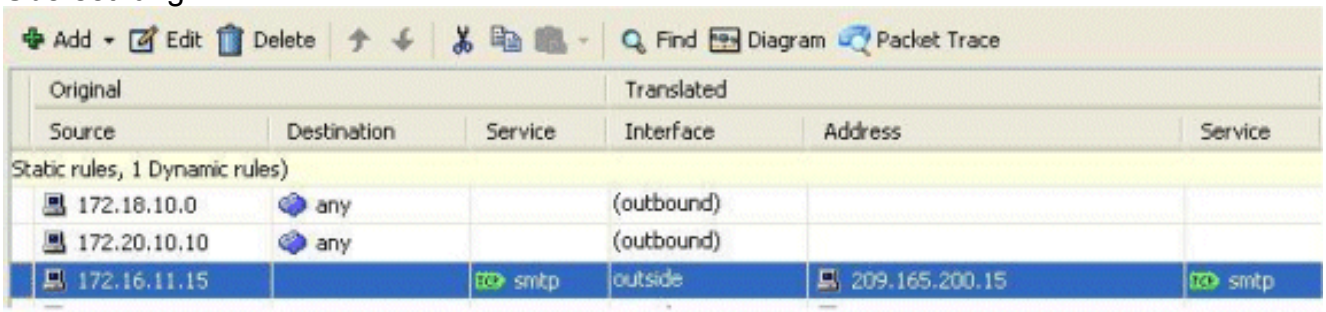
Gehen Sie wie folgt vor:

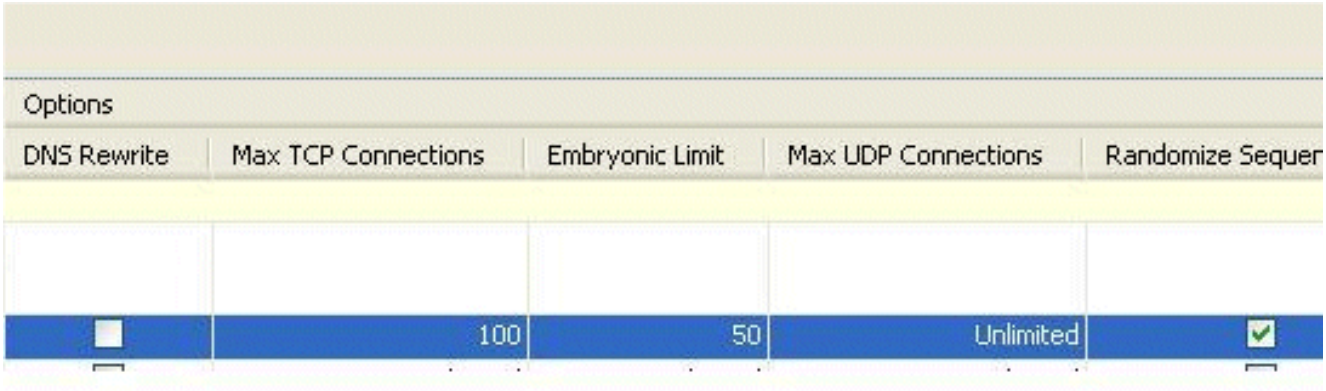
1. Klicken Sie auf die Registerkarte **Verbindungseinstellungen**, und geben Sie die Werte für die maximalen Verbindungen für diese statische Übersetzung



an.

2. Diese Bilder zeigen die Verbindungsgrenzen für diese spezifische statische Übersetzung:





Dies ist die entsprechende CLI-Ausgabe:

```
!
static (inside,outside) TCP 209.165.200.15 smtp 172.16.11.15 smtp netmask
    255.255.255.255 TCP 100 50
!
```

Zeitbasierte Zugriffsliste

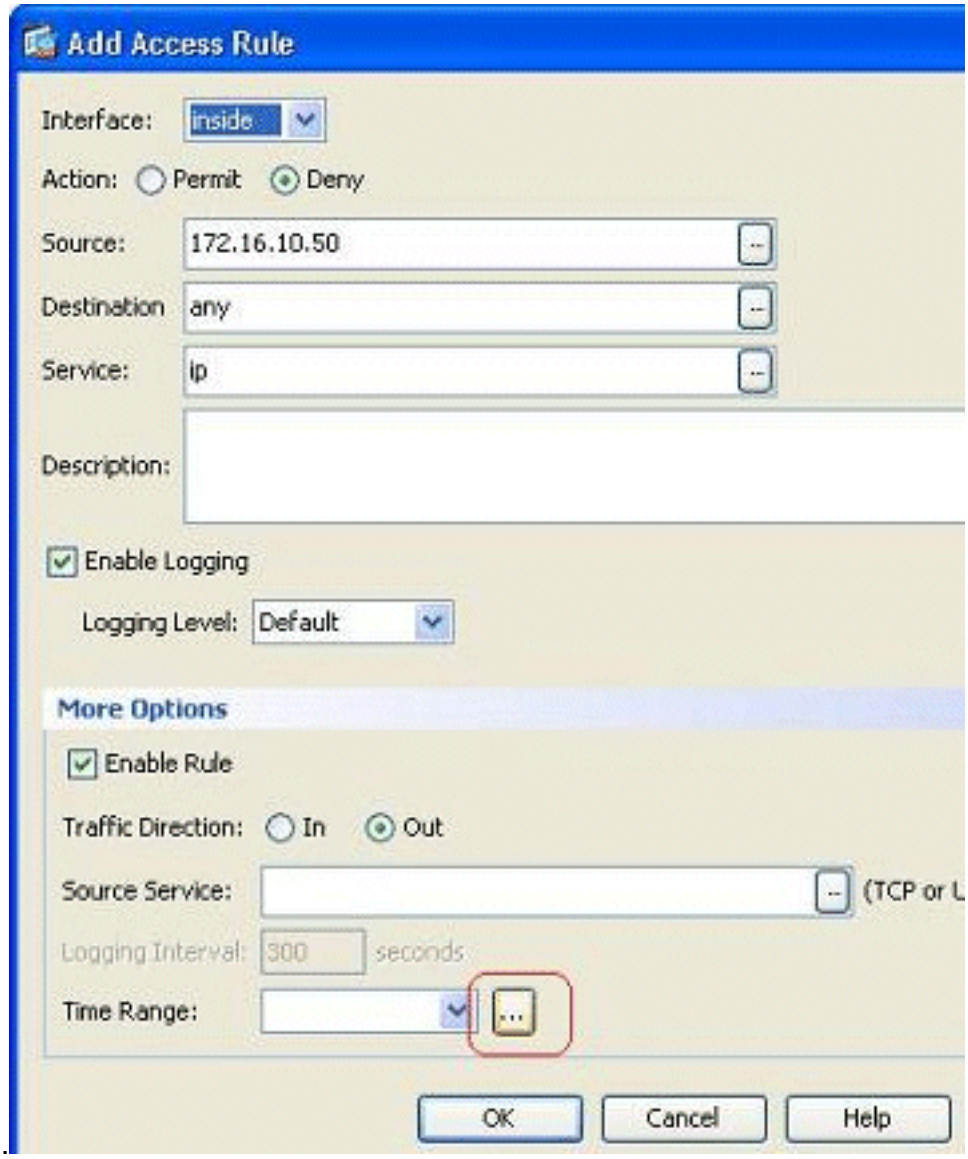
Dieser Abschnitt behandelt die Implementierung zeitbasierter Zugriffslisten mithilfe des ASDM. Zugriffsregeln können je nach Zeit angewendet werden. Um dies zu implementieren, müssen Sie einen Zeitraum definieren, der die Zeitangaben nach Tag, Woche, Monat oder Jahr angibt. Anschließend müssen Sie diesen Zeitraum an die erforderliche Zugriffsregel binden. Der Zeitbereich kann auf zwei Arten definiert werden:

1. Absolut - Definiert einen Zeitraum mit Startzeit und Endzeit.
2. Periodic (Periodisch) - Wird auch als periodisch bezeichnet. Definiert einen Zeitraum, der in angegebenen Intervallen auftritt.

Hinweis: Stellen Sie vor dem Konfigurieren des Zeitbereichs sicher, dass die ASA mit den richtigen Datums-/Uhrzeiteinstellungen konfiguriert wurde, da diese Funktion die Systemuhr-Einstellungen für die Implementierung verwendet. Die Synchronisierung der ASA mit dem NTP-Server führt zu deutlich besseren Ergebnissen.

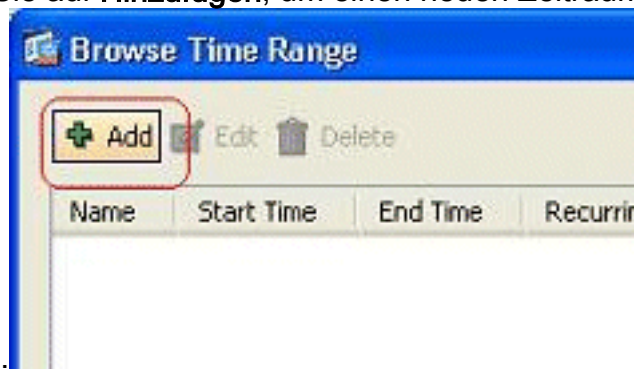
Gehen Sie wie folgt vor, um diese Funktion über ASDM zu konfigurieren:

1. Klicken Sie beim Definieren der Zugriffsregel auf die Schaltfläche **Details** im Feld



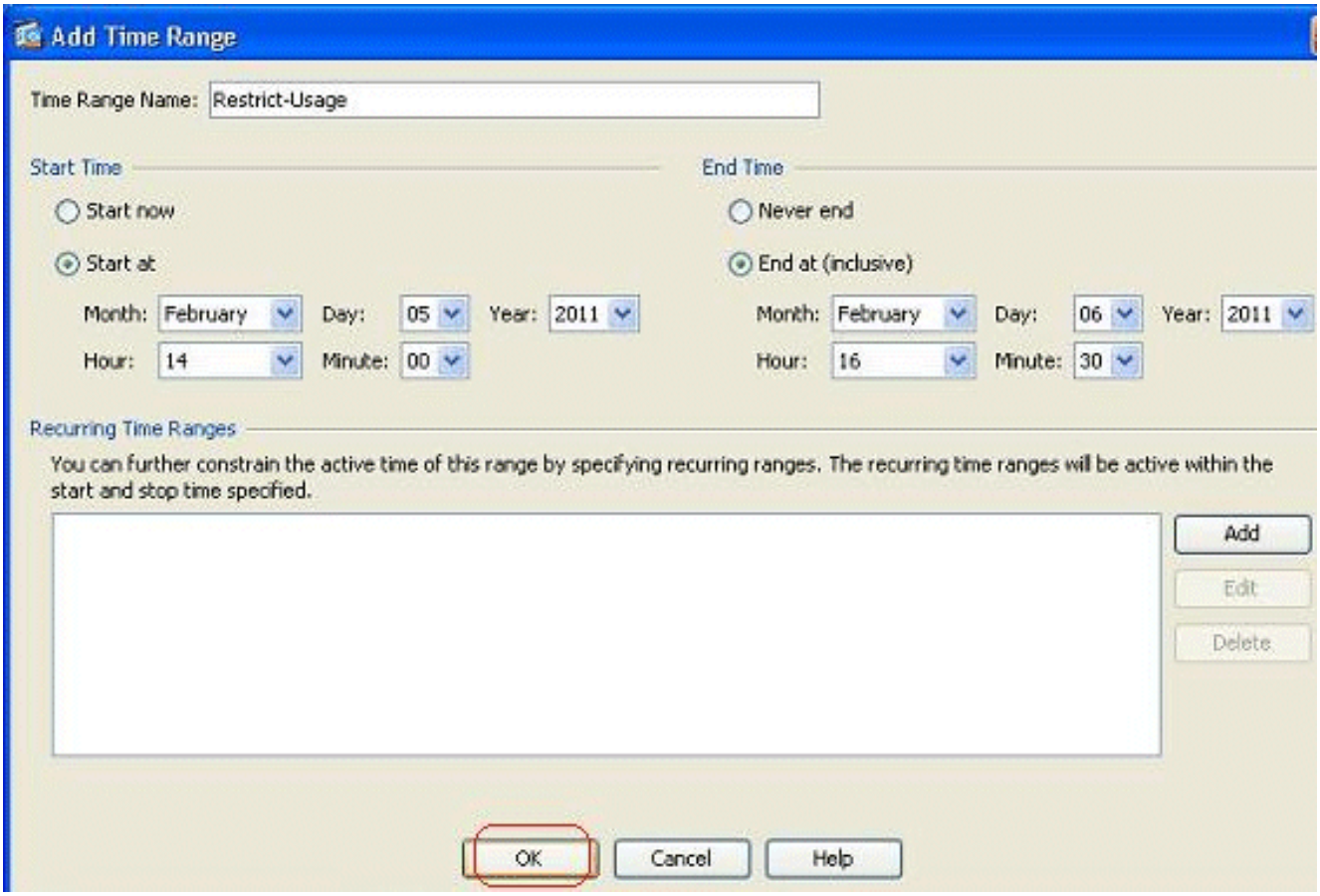
Zeitbereich.

2. Klicken Sie auf **Hinzufügen**, um einen neuen Zeitraum zu

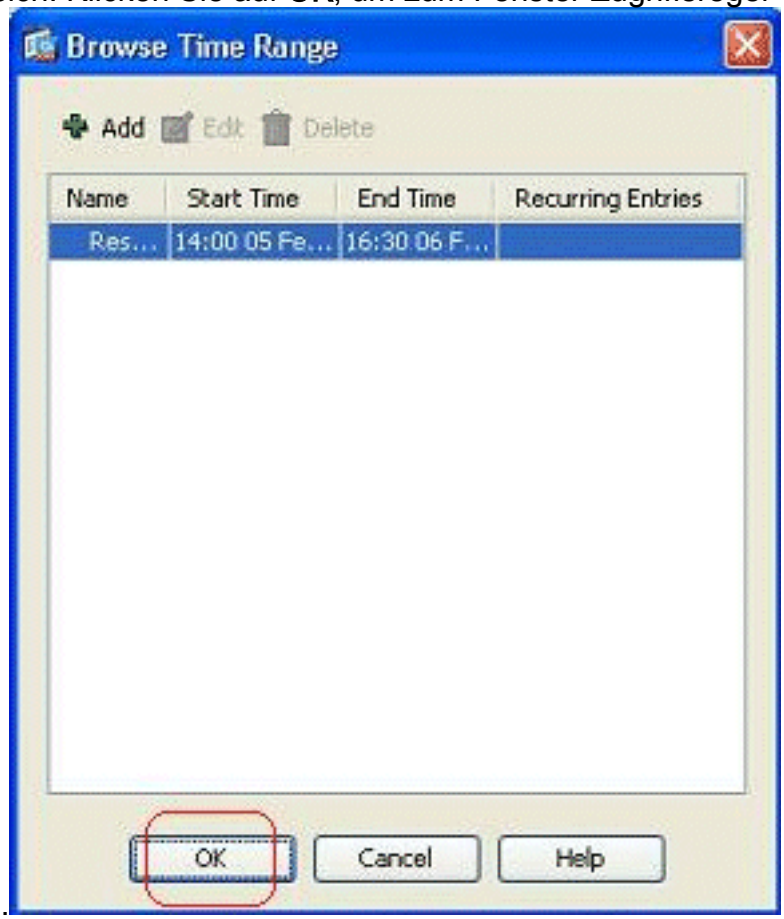


erstellen.

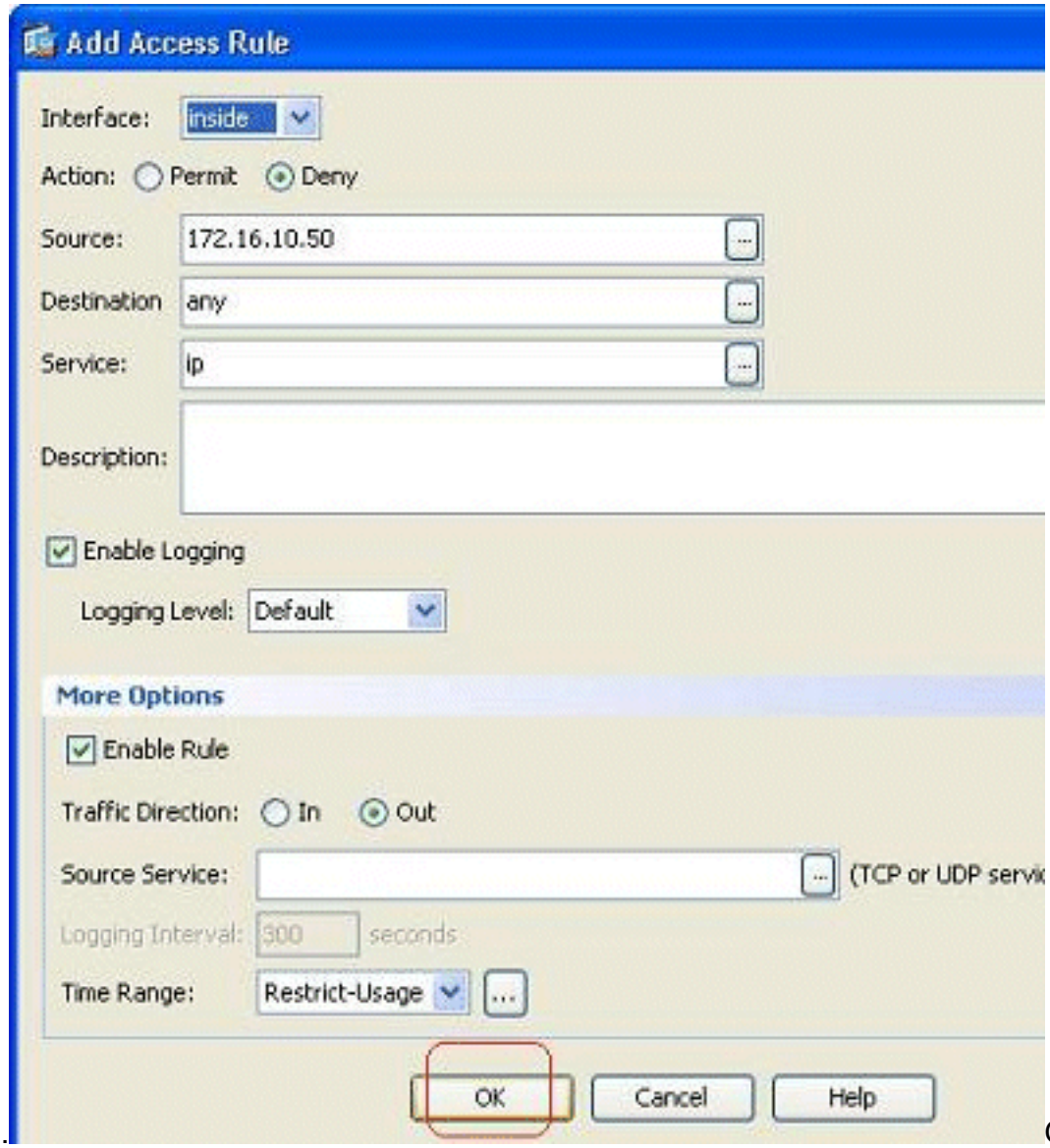
3. Definieren Sie den Namen des Zeitbereichs, und geben Sie die Startzeit und Endzeit an. Klicken Sie auf **OK**.



4. Hier sehen Sie den Zeitbereich. Klicken Sie auf **OK**, um zum Fenster Zugriffsregel hinzufügen zurückzukehren.



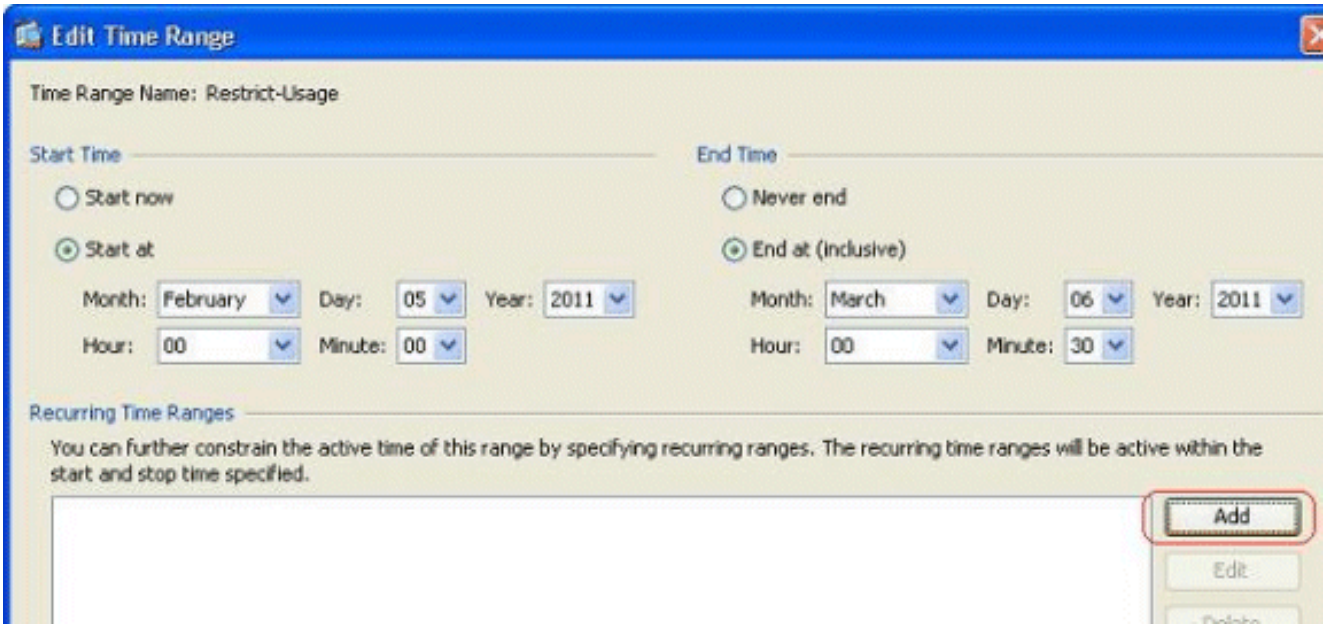
5. Sie können jetzt sehen, dass der Zeitbereich Beschränkung der Nutzung an diese Zugriffsregel gebunden



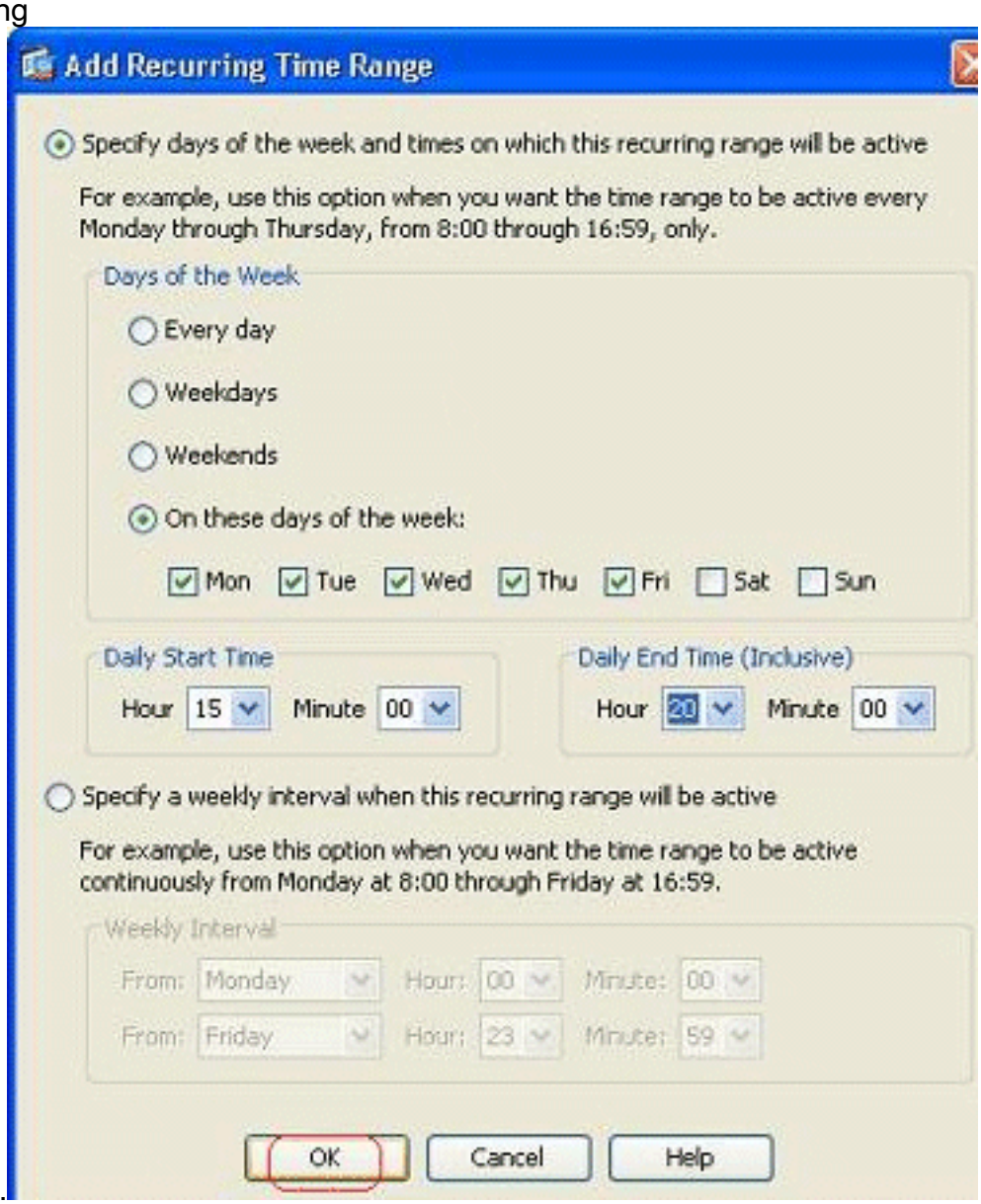
wurde. Gemäß dieser Zugriffsregelkonfiguration ist der Benutzer von 172.16.10.50 auf die Verwendung von Ressourcen vom 05.02.2011, 14.06.2011, 16.30 Uhr, beschränkt. Dies ist die entsprechende CLI-Ausgabe:

```
time-range Restrict-Usage
 absolute start 14:00 05 February 2011 end 16:30 06 February 2011
!
access-list inside_access_out extended deny ip host 172.16.10.50 any
    time-range Restrict-Usage
!
access-group inside_access_out in interface inside
```

6. Im Folgenden finden Sie ein Beispiel zum Angeben eines sich wiederholenden Zeitbereichs. Klicken Sie auf **Hinzufügen**, um einen sich wiederholenden Zeitraum zu definieren.

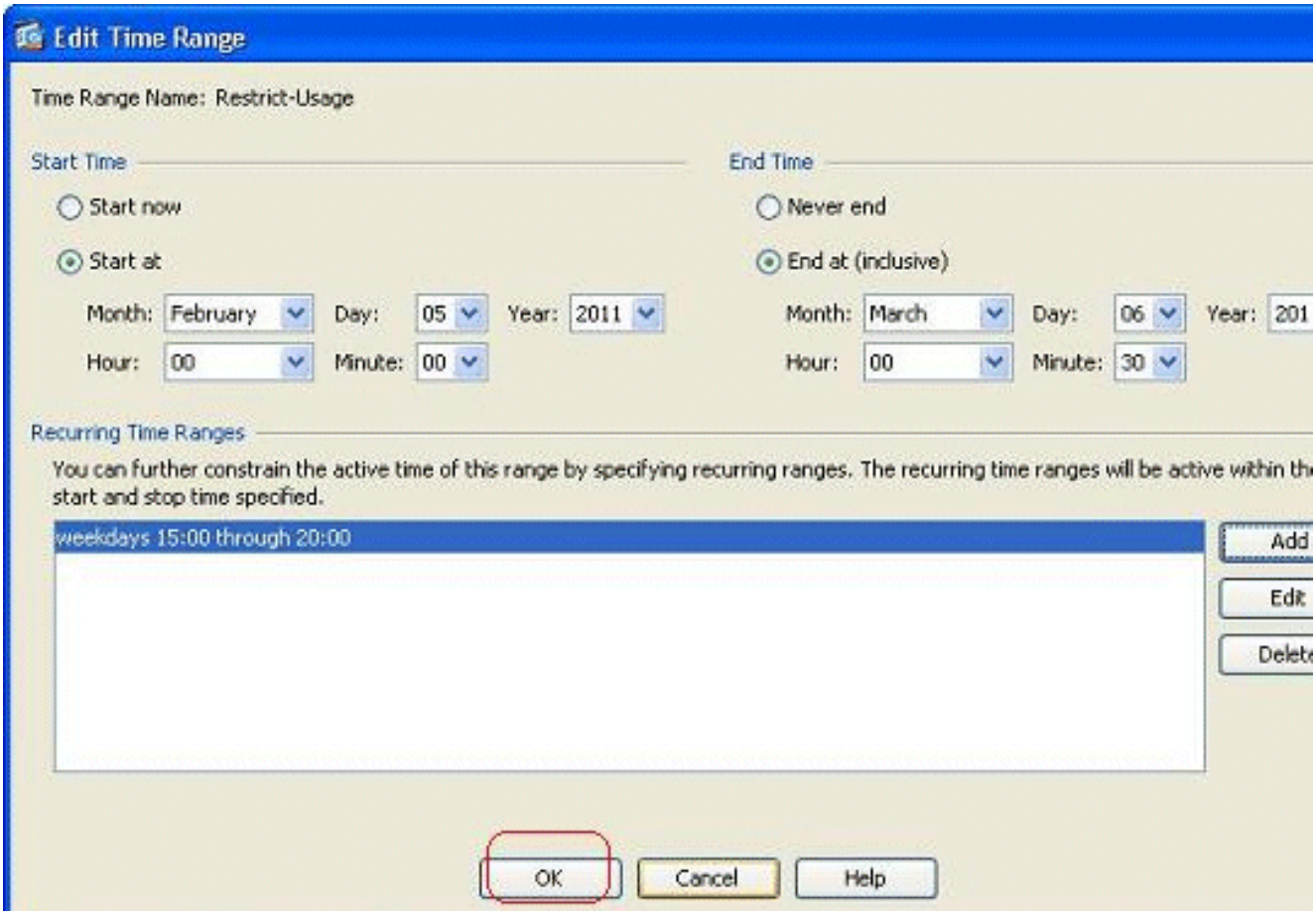


7. Geben Sie die Einstellungen entsprechend Ihren Anforderungen an, und klicken Sie auf **OK**, um den Vorgang



abzuschließen.

8. Klicken Sie auf **OK**, um zum Fenster Zeitbereich zurückzukehren.



Laut dieser Konfiguration wurde dem Benutzer am 17.16.10.50 von 15:00 bis 20:00 Uhr an allen Wochentagen außer Samstag und Sonntag der Zugriff auf Ressourcen verweigert.

```
!
time-range Restrict-Usage
 absolute start 00:00 05 February 2011 end 00:30 06 March 2011
 periodic weekdays 15:00 to 20:00
!
access-list inside_access_out extended deny ip host 172.16.10.50 any
    time-range Restrict-Usage
!
access-group inside_access_out in interface inside
```

Hinweis: Wenn ein **Zeitbereichsbefehl** sowohl absolute als auch periodische Werte angegeben hat, werden die **periodischen** Befehle erst nach Erreichen der absoluten Startzeit ausgewertet und nach Erreichen der absoluten Endzeit nicht weiter ausgewertet.

Zugehörige Informationen

- Cisco ASA-Dokumentationsseite
- Technischer Support und Dokumentation - Cisco Systems